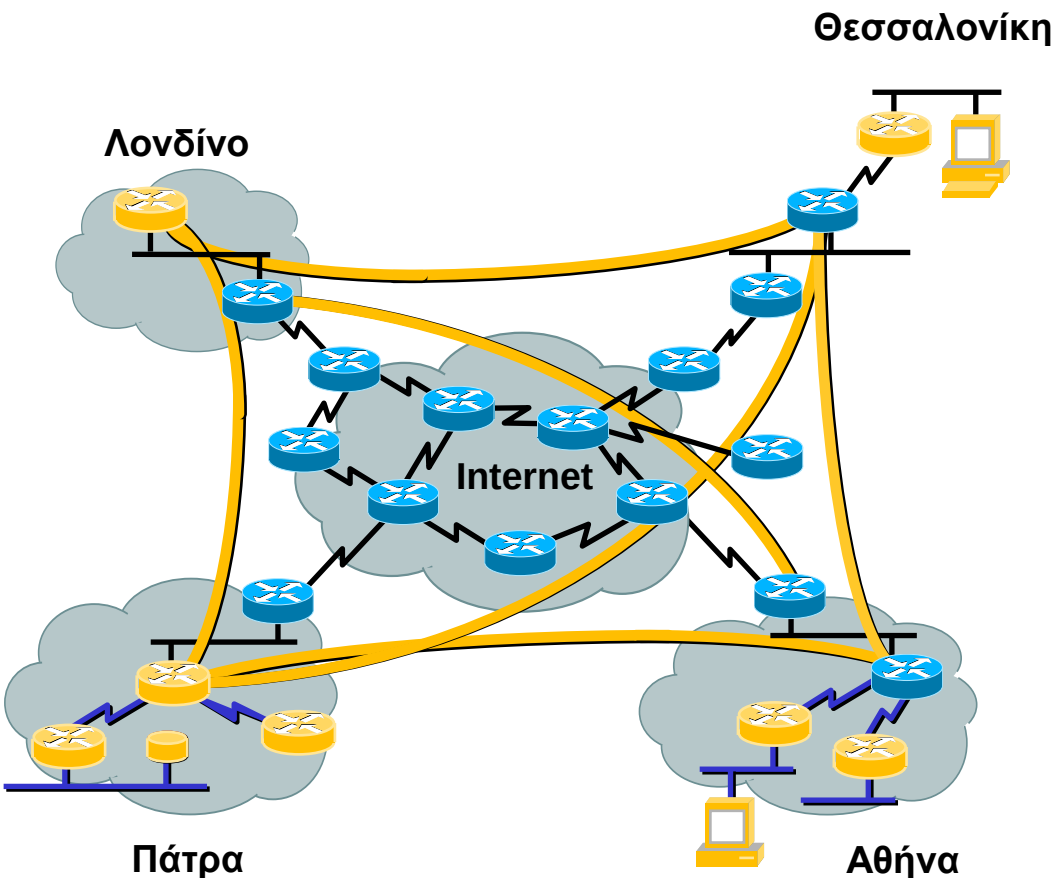
ΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΟΥ ΦΟΙΤΗΤΗ *ΙΩΑΝΝΗ ΣΑΛΑΜΟΥ*

ΘΕΜΑ ΕΡΓΑΣΙΑΣ:

*Εικονικά Ιδιωτικά Δίκτυα VPN(*Virtual Private Networks)



ΠΕΡΙΕΧΟΜΕΝΑ

1.ΕΙΣΑΓΩΓΗ

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.

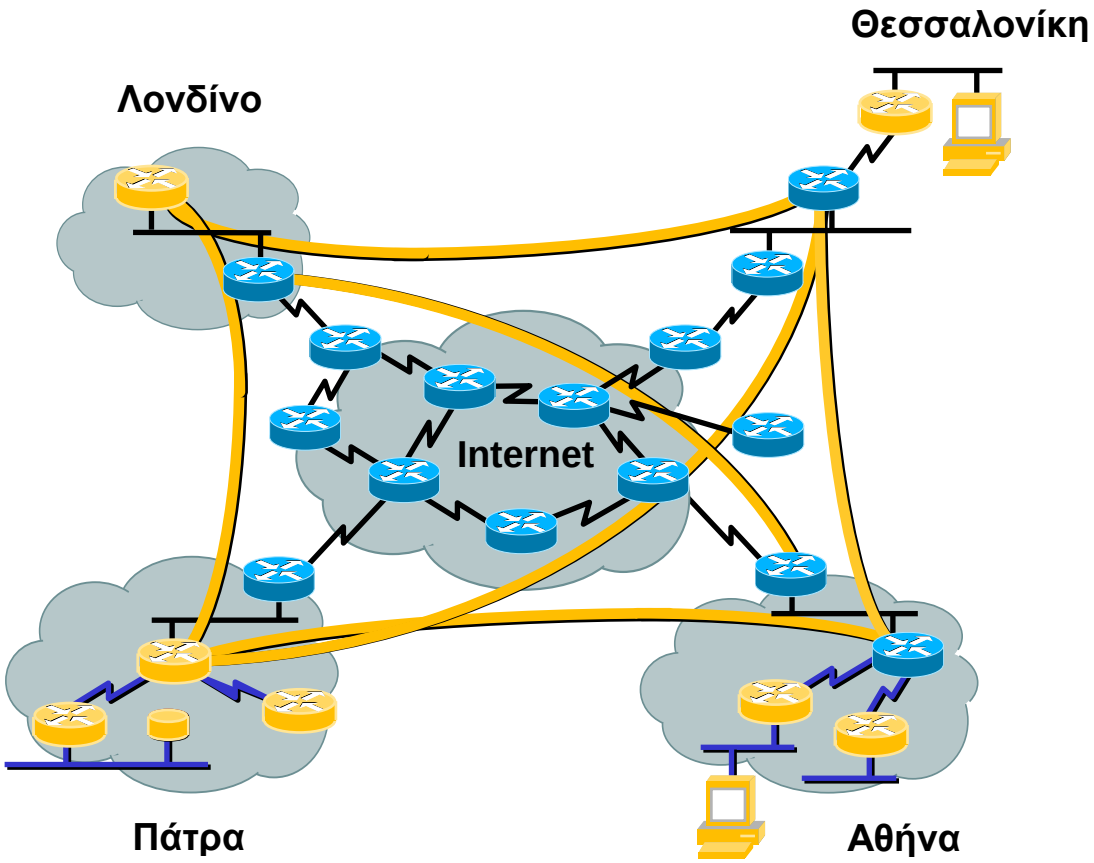
2. Ιστορική αναδρομή – Αρχιτεκτονικές των VPNs

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»

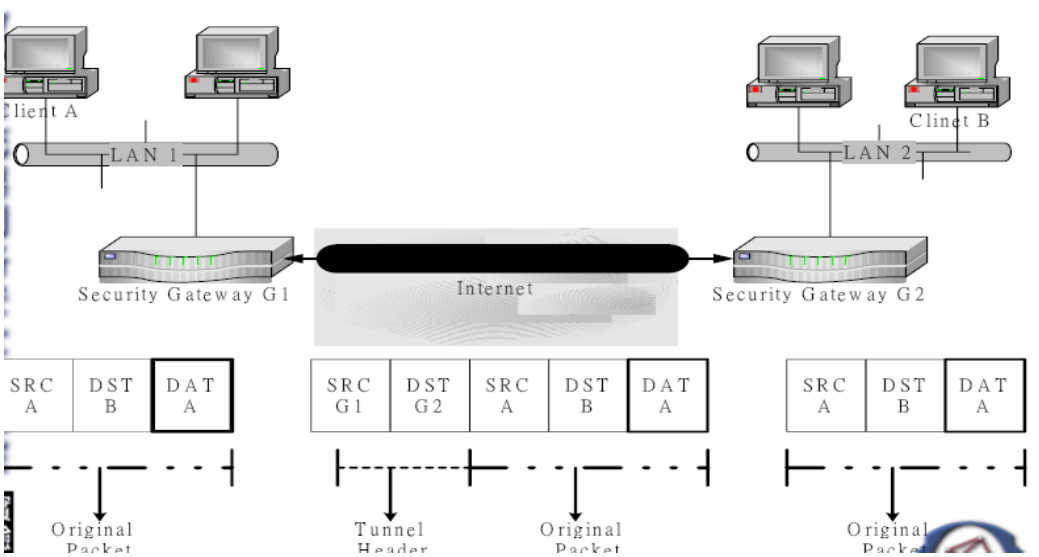
b. Τα VPN δομής «δίκτυο-προς-δίκτυο» (LAN-to-LAN), όπου η δίοδος μεταφοράς των δεδομένων αναπτύσσεται μεταξύ δύο τοπικών δικτύων.

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.

3. 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.

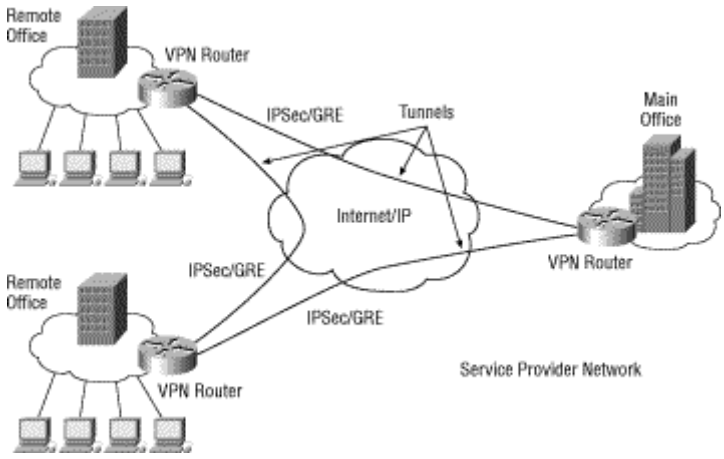
Η εγκαθίδρυση «διόδου» (tunneling) είναι η τεχνική ενθυλάκωσης ενός ολόκληρου πακέτου/πλαισίου δεδομένων σε ένα πακέτο/πλαίσιο διαφορετικού πρωτοκόλλου. Η επικεφαλίδα του tunneling πρωτοκόλλου προσαρτάται στο αρχικό πακέτο ενώ η μεταφορά/μετάδοση πραγματοποιείται με χρήση του νέου πρωτοκόλλου. Έτσι, 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 2: 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 πρόκειται 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 3: 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.

3.1 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.

3.2 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

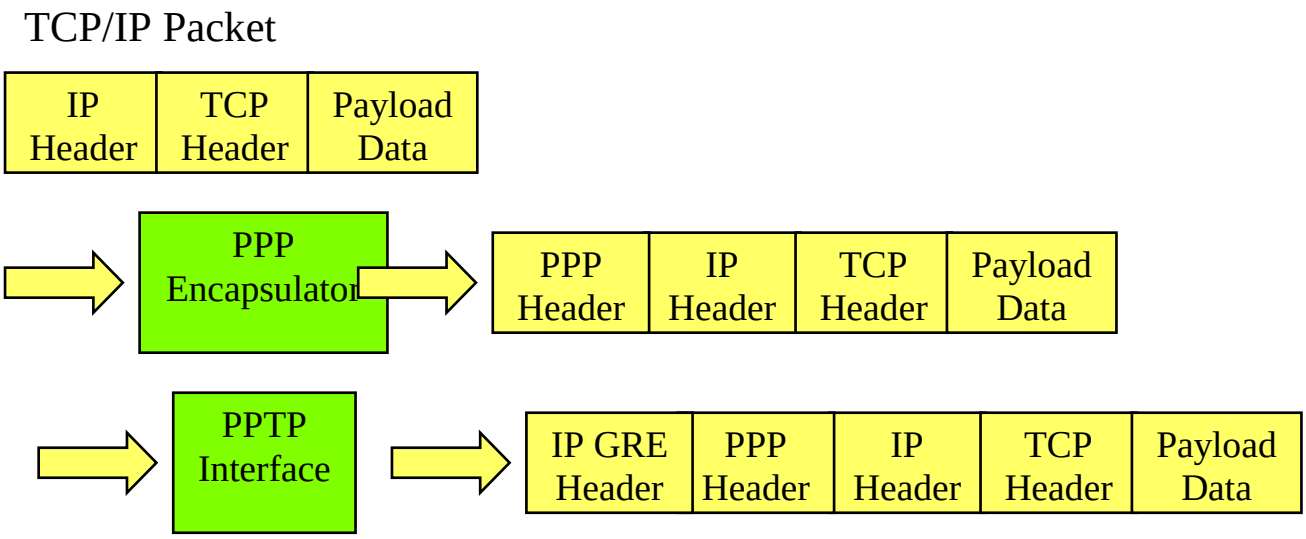
καινούριο IP πακέτο για μεταφορά. Για την πιστοποίηση της ταυτότητας του χρήστη χρησιμοποιεί τους μηχανισμούς PAP ή CHAP που παρέχονται από το PPP. Χρησιμοποιεί το Generic Routing Protocol (GRE) για μεταφορά των PPP πακέτων. Πραγματοποιεί επίσης κρυπτογράφηση για τα ενθυλακωμένα δεδομένα.

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 4).



Σχήμα 4: 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.

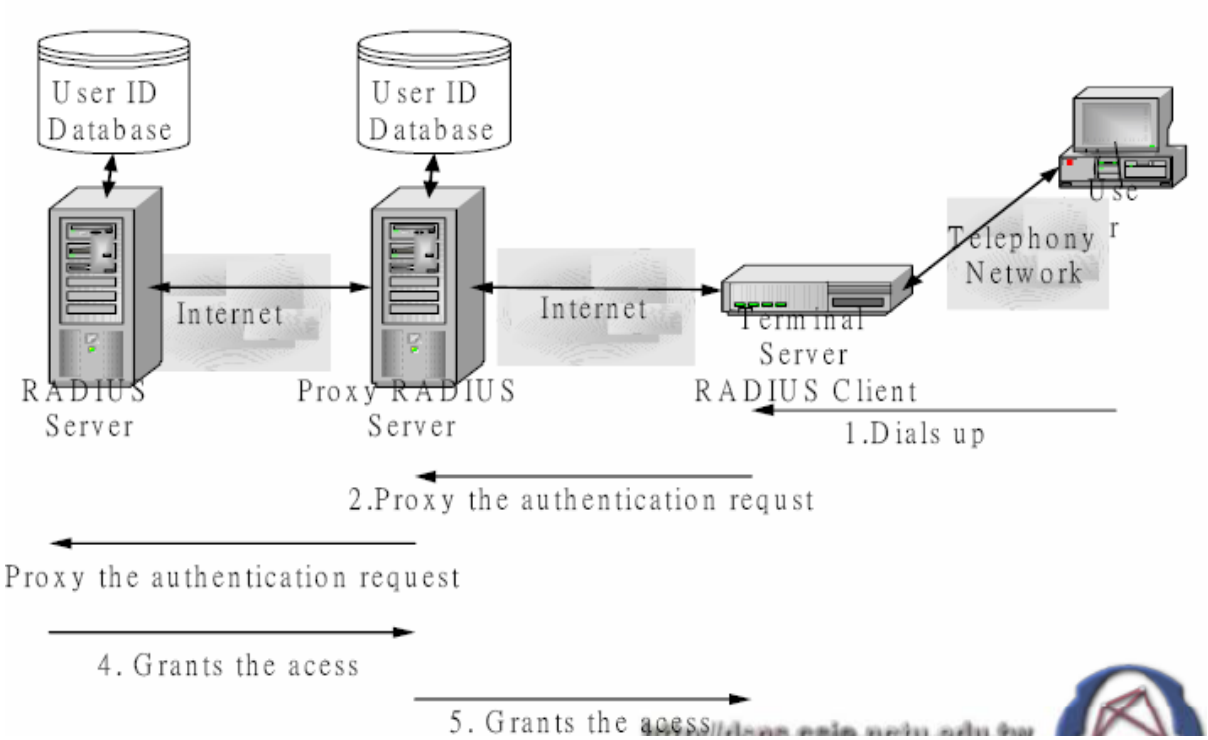
Μία από τις βασικές λειτουργίες του NAS είναι η πιστοποίηση ταυτότητας του χρήστη (δηλαδή ο έλεγχος του κατά πόσον ο χρήστης είναι εξουσιοδοτημένος στο να συνδεθεί στο δίκτυο). Αυτός ο έλεγχος ταυτότητας γίνεται μετά την αρχική αίτηση σύνδεσης στον ISP, κατά την οποία η ταυτότητα του χρήστη επικυρώθηκε 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 5).

Στο PPTP, οι ζεύξεις επικοινωνίας υλοποιούνται πάνω σε διόδους (tunnels)(σχήμα 6). 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.

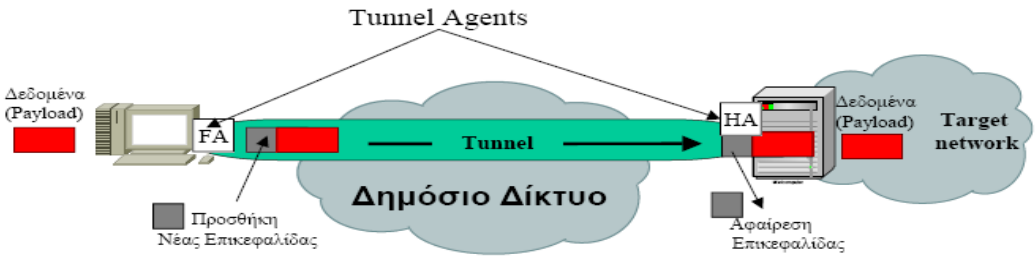


Σχήμα 5: Λειτουργία του RADIUS με Proxy Server

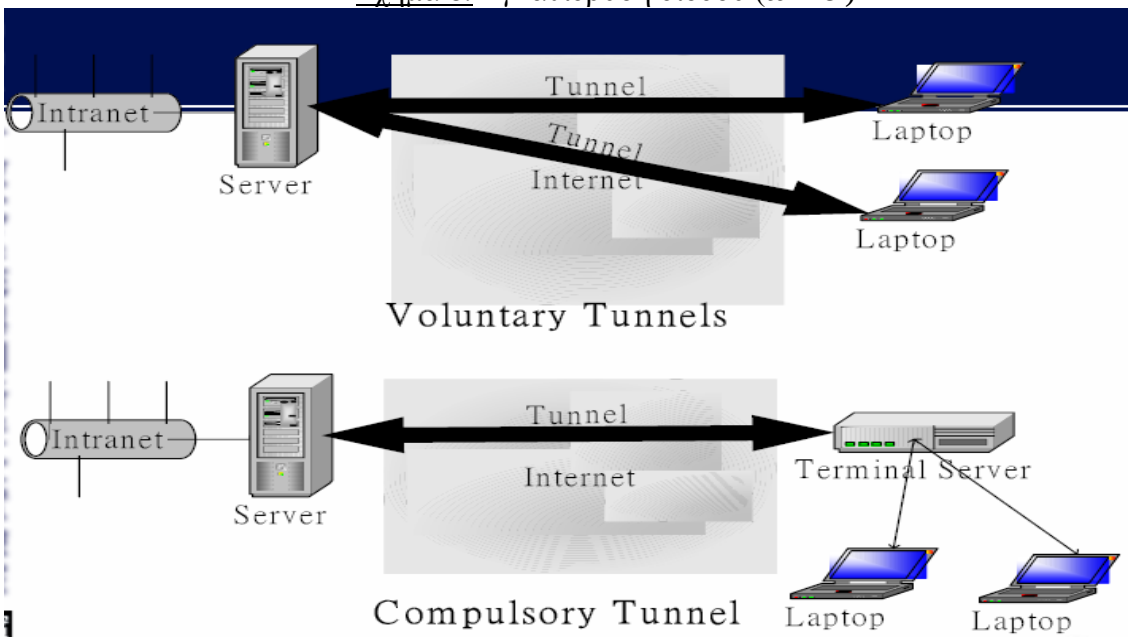
Υπάρχουν δύο ειδών δίοδοι: οι **«αυθόρμητες» δίοδοι (mandatory tunnels)** και οι **«αναγκαστικές» δίοδοι (compulsory ή mandatory tunnels)**. Οι πρώτες δημιουργούνται μετά από αίτηση του χρήστη, ενώ οι αναγκαστικές δίοδοι δημιουργούνται αυτόματα, χωρίς καμία παρεμβολή από τον χρήστη.

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 6: Εγκαθίδρυση διόδου (tunnel)



Σχήμα 7: 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).

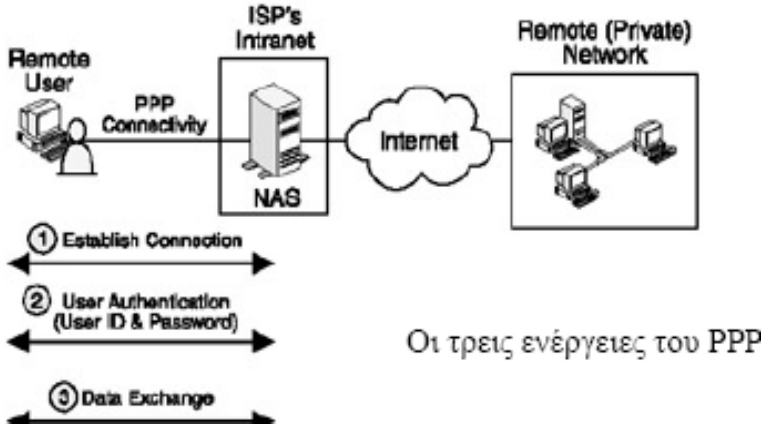
  Γενικότερα, οι στατικές δίοδοι δεν προσφέρονται σε συστήματα όπου υπάρχει μεγάλο πλήθος χρηστών που αιτούνται πρόσβαση.

- 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 8).
- 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

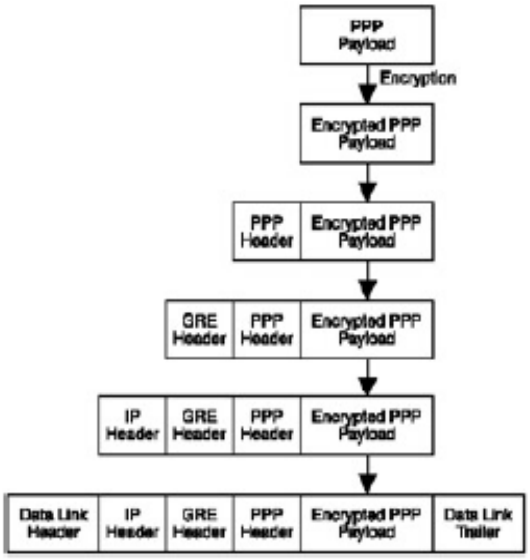
προκύπτει από εφαρμογή μιας συνάρτησης κατακερματισμού στο password του χρήστη (αφού το password το έχει, εκτός βέβαια από τον ίδιο το χρήστη, και το δίκτυο λόγω του RADIUS Server, δεν χρειάζεται ανταλλαγή κλειδιού). Η κρυπτογράφηση ξεκινά από τον υπολογιστή του χρήστη – κάτι που προσδίδει μεγαλύτερη 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.



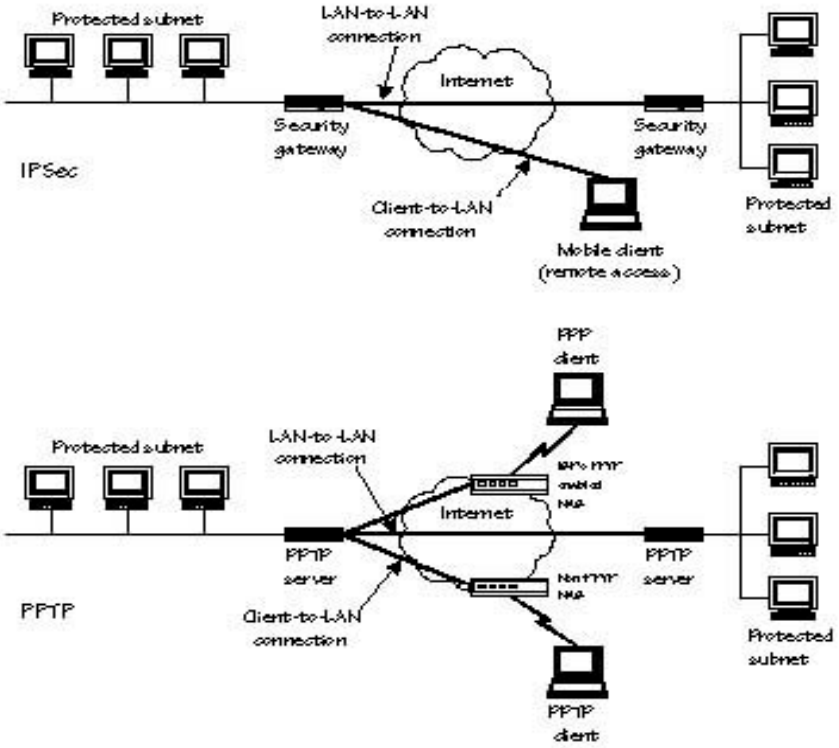
Σχήμα 8: Η πρώτη φάση του PPTP (χρήση του PPP, το οποίο λειτουργεί με 3 στάδια)

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 9). 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 9: Ενθυλάκωση ενός πακέτου δεδομένων στο PPTP



Σχήμα 10: 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).

3.3 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:

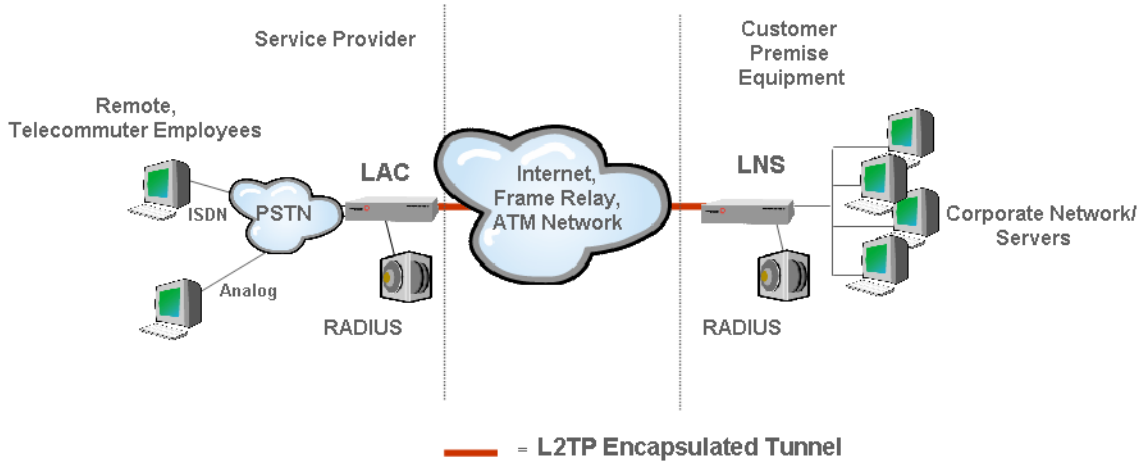
- τον **LAC (L2TP Access Concentrator)** – Βρίσκεται στον ISP και χρησιμοποιείται για την εγκαθίδρυση μίας διόδου σε ένα δημόσιο δίκτυο π.χ. PSTN, ISDN, η οποία τερματίζεται στον LNS του κόμβου προορισμού

- 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 11:



Σχήμα 11: 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. 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.

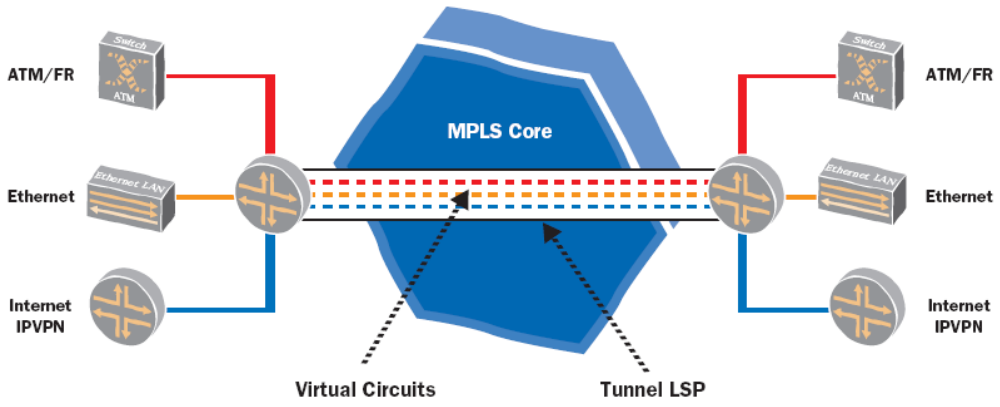
Τέλος, θα πρέπει να σημειωθεί ότι το L2TP πρωτόκολλο μπορεί να χρησιμοποιηθεί και για σύνδεση δίκτυο-προς-δίκτυο (LAN-to-LAN tunneling): ειδική μέριμνα πρέπει να υπάρξει ώστε κάθε άκρο της διόδου να μπορεί να δρα ταυτόχρονα και σαν LAC αλλά και σαν LNS.

3.4 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 12: 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-

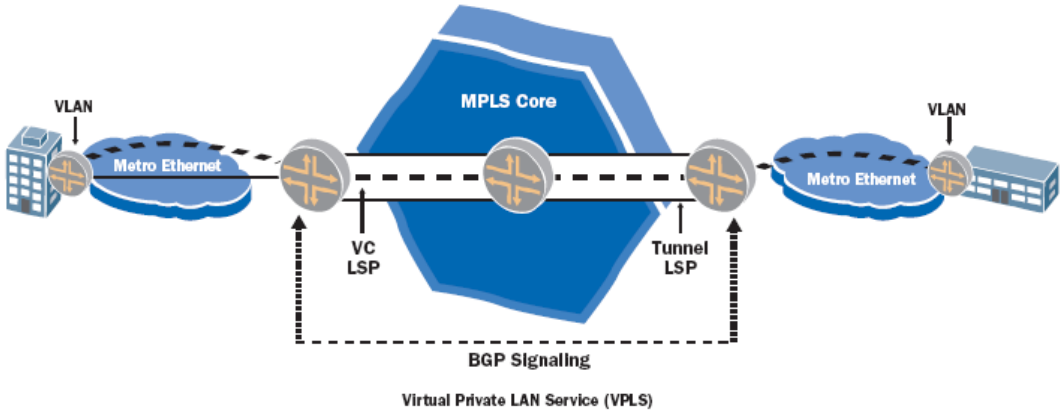
Kompella VPN χρησιμοποιούν το πρωτόκολλο BGP και όχι το LDP για τη δημιουργία των διόδων. Το πλεονέκτημα είναι ότι το BGP ήδη χρησιμοποιείται και για την υλοποίηση των L3 VPNs που μπορεί να συνυπάρχουν στο δίκτυο κορμού - επομένως δεν απαιτείται η εισαγωγή ενός ακόμη πρωτοκόλλου όπως είναι το LDP.

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.

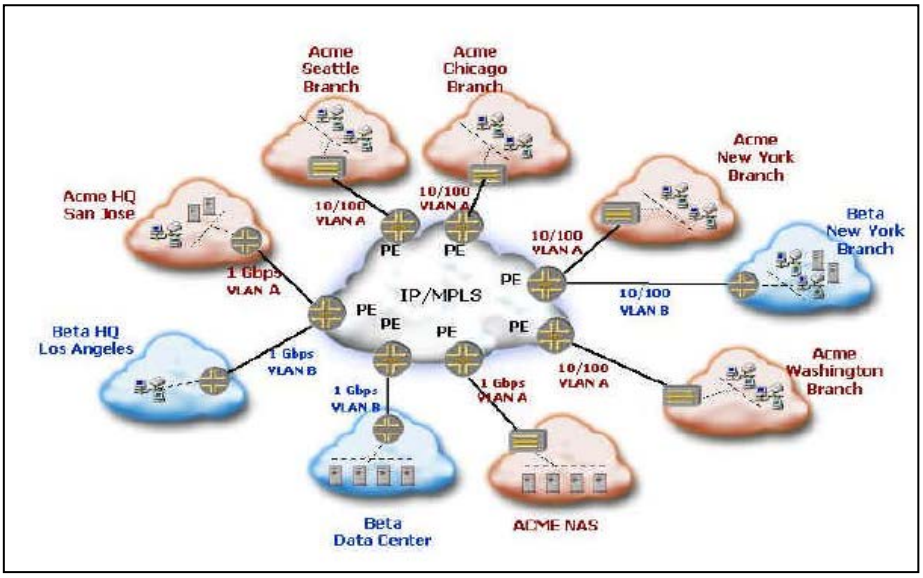
Χαρακτηριστικό είναι και το σχήμα που ακολουθεί:



Σχήμα 13: 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 14: 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.

4.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.

4.1 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.

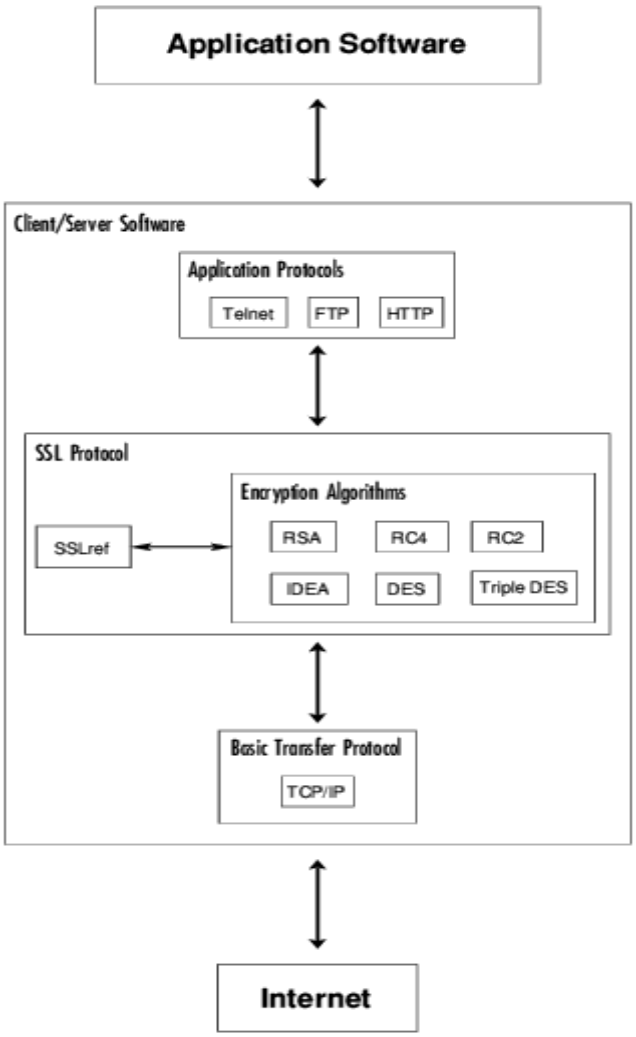
Διευκρινίζεται ότι τα SSL VPNs αφορούν εφαρμογές που υποστηρίζουν το πρωτόκολλο SSL, όπως για παράδειγμα Web browsers και Web-based e-mail.

4.2 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.



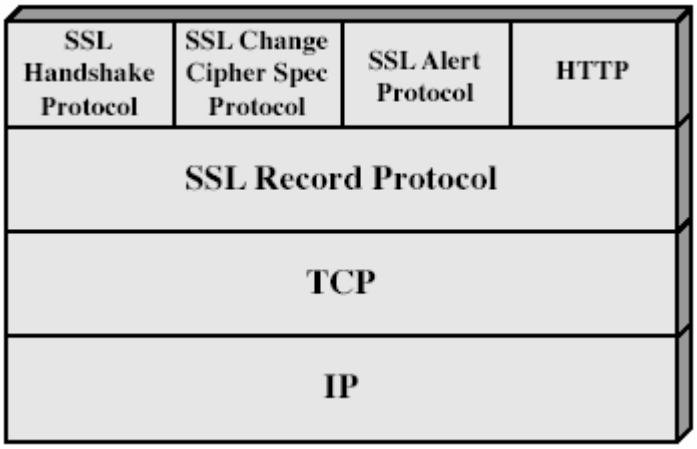
Σχήμα 15: Αναπαράσταση του πρωτοκόλλου SSL

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 16:



Σχήμα 16: 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

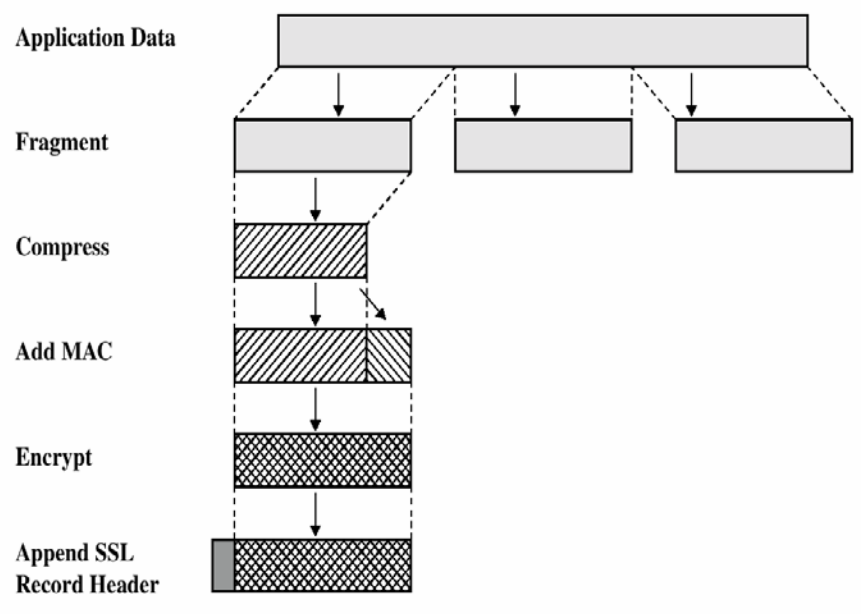
κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

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 17.



Σχήμα 17: 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 εξυπηρέτησης 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.

4.3 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.ΤΥΠΙΚΕΣ ΤΟΠΟΛΟΓΙΕΣ VPN

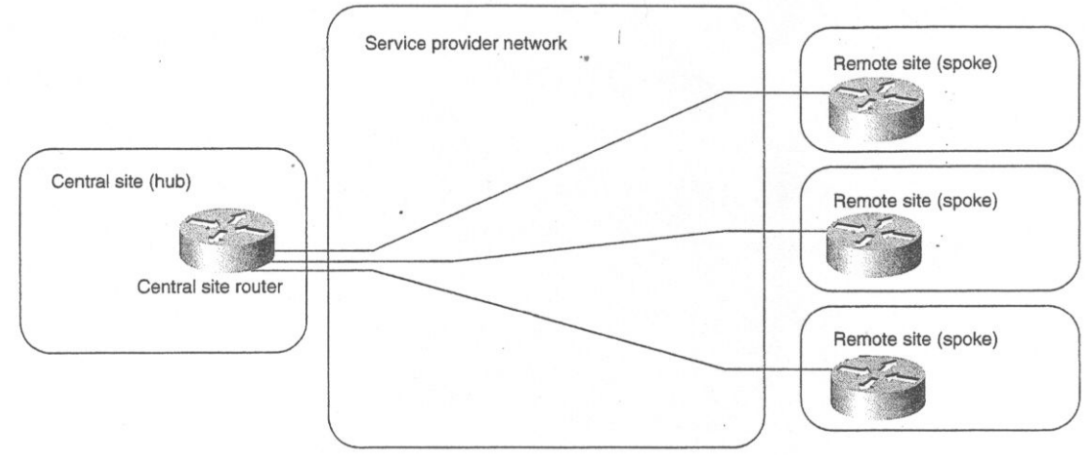
Η VPN τοπολογία που απαιτείται από έναν οργανισμό πρέπει να καλύπτει τις απαιτήσεις της επιχείρησης. Παρόλα αυτά, υπάρχουν διάφορες πολύ γνωστές τοπολογίες που αξίζει να αναφερθούν. Οι ίδιες τοπολογίες μπορούν να λύνουν μια ποικιλία από διαφορετικά θέματα επιχείρησης ανάλογα με τις απαιτήσεις ης αγοράς αλλά και του επιχειρηματικού κλάδου στον οποίο δραστηριοποιούνται.
Οι VPN τοπολογίες που θα περιγραφούν μπορούν να διαιρεθούν σε τρεις ,μεγάλες κατηγορίες.

• Τοπολογίες επηρεασμένες από το Overlay VPN μοντέλο. Συγκεκριμένα προκειται για τις:
Hub and Spoke τοπολογίες, partial ή full mesh τοπολογία και hybrid τοπολογία.
• Extranet τοπολογίες, και συγκεκριμένα τα any-to-any Extranet και Central Services Extranet
• Ειδικού σκοπού (Special Purpose) τοπολογίες, όπως οι VPDN backbone και Manager Network τοπολογία

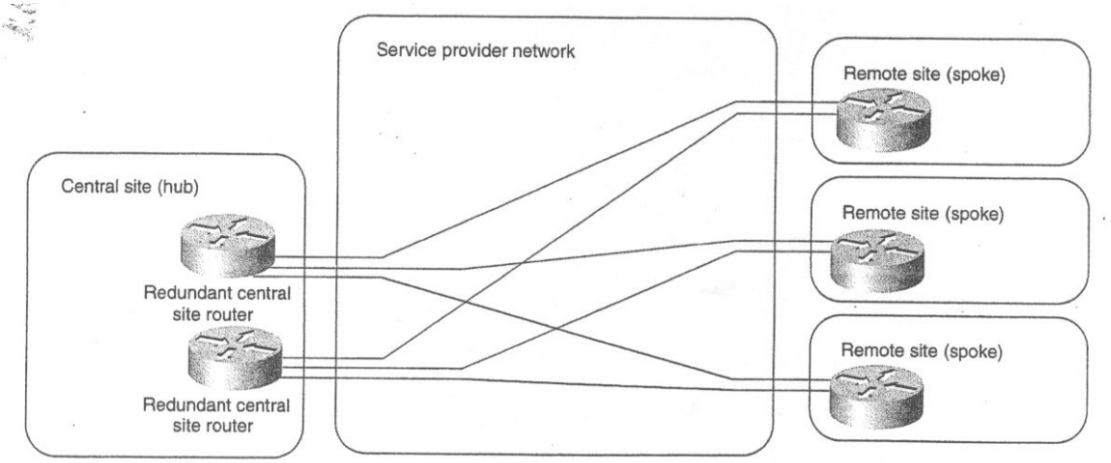
5.1 Τοπολογία Hub-and-spoke

Η τοπολογία που συνιστάται περισσότερο είναι η hub and spoke τοπολογία, όπου ένας αριθμός από απομακρυσμένα γραφεία (spokes), είναι συνδεδεμένα σε μια κεντρική τοποθεσία(hub) όμοια με το σενάριο στο Σχήμα 17 Τα απομακρυσμένα γραφεία μπορούν να ανταλλάσσουν δεδομένα (συνήθως δεν υπάρχουν αυστηροί περιορισμοί ασφαλείας στην ανταλλαγή δεδομένων εσωτερικά στα γραφεία), αλλά το σύνολο των ανταλλασόμενων δεδομένων μεταξύ αυτών είναι αμελητέο.

Η τοπολογία hub and spoke συχνά χρησιμοποιείται σε οργανισμούς με αυστηρές ιεραρχικές δομές, για παράδειγμα: σε τράπεζες, κυβερνήσεις ή διεθνείς οργανισμούς με περιορισμένα ανά χώρα γραφεία. Για τη κάλυψη των αυξημένων απαιτήσεων σε επικαλυπτόμενες συνδέσεις, στην απλή hub and spoke τοπολογία (Σχήμα 18),συχνά προστίθεται ένας επιπρόσθετος δρομολογητής στην κεντρική τοποθεσία (Σχήμα 19), ή ένα κεντρικό site που χρησιμοποιείται σαν αντίγραφο, το οποίο σε αυτή τη περίπτωση είναι συνδεδεμένο με το πρωτεύον κεντρικό δίκτυο μέσα από μια σύνδεση μεγαλύτερης ταχύτητας.



Σχήμα 18 Hub and spoke τοπολογία



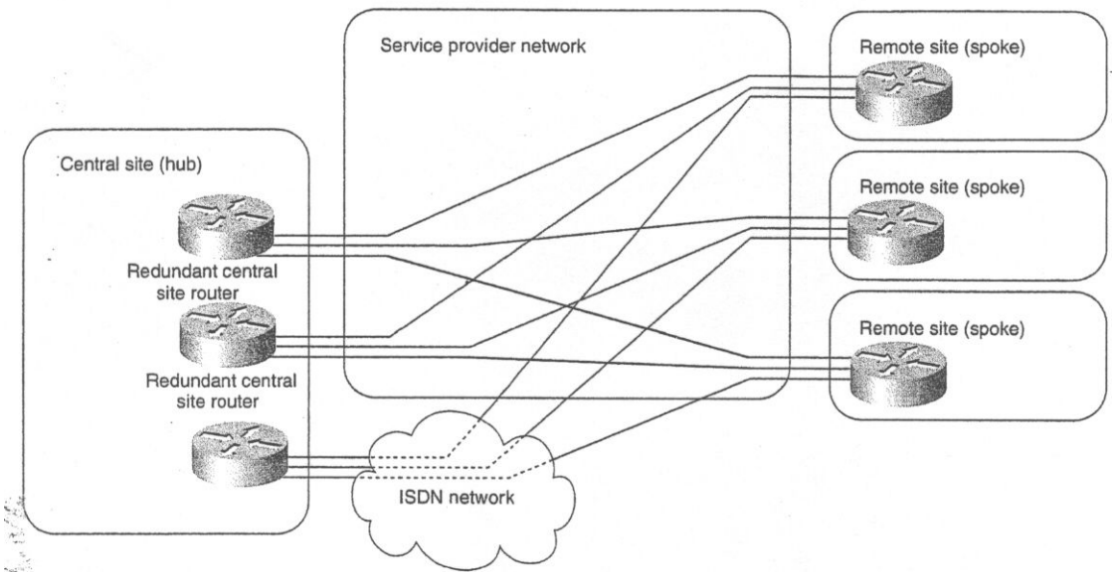
Σχήμα 19 Hub and spoke τοπολογία με δύο κεντρικούς δρομολογητές

Η υλοποίηση πλεονάζουσας (redundant) hub and spoke τοπολογίας με Overlay VPNμοντέλο βασισμένο σε VC, παρουσιάζει μια σειρά από προκλήσεις. Κάθε spoke τοποθεσία απαιτεί ένα VC προς τουλάχιστον δύο κεντρικούς δρομολογητές. Αυτά τα VCs μπορούν να είναι παρέχονται στη λογική της primary-backup διάταξης ή σε μια διάταξη διαμοιραζόμενου φορτίου λύσεις που έχουν μια σειρά από προβλήματα όπως:

1. Στη διάταξη primary-backup, το εφεδρικό (back-up) VC είναι αχρησιμοποίητο ενώ το πρωτεύον VC είναι ενεργό, έχοντας σαν αποτέλεσμα πλεονάζουσες δαπάνες από τον πελάτη.
2. Στη διάταξη διαμοιραζόμενου φορτίου, η hub and spoke τοποθεσία αντιμετωπίζει μειωμένο throughput εάν ένα από τα VCs (ή ένας από τους κεντρικούς δρομολογητές) αποτύχει.Οι πάροχοι υπηρεσιών υψηλής ποιότητας προσπαθούν να ικανοποιήσουν τις απαιτήσεις των πελατών τους για εφεδρικές συνδέσεις με προηγμένες υπηρεσίες που προσφέρουν shadow PVCs. Με το shadow PVC ο πελάτης παίρνει δύο εικονικά κυκλώματα στην τιμή του ενός, στην περίπτωση όπου μπορούν να χρησιμοποιήσουν μόνο μια VC για κίνηση δεδομένων. Ένα μικρό σύνολο της κίνησης αφήνεται στη δεύτερη PVC ώστε να επιτρέψει αλλαγές πρωτοκόλλου δρομολόγησης πάνω στη δεύτερη PVC.

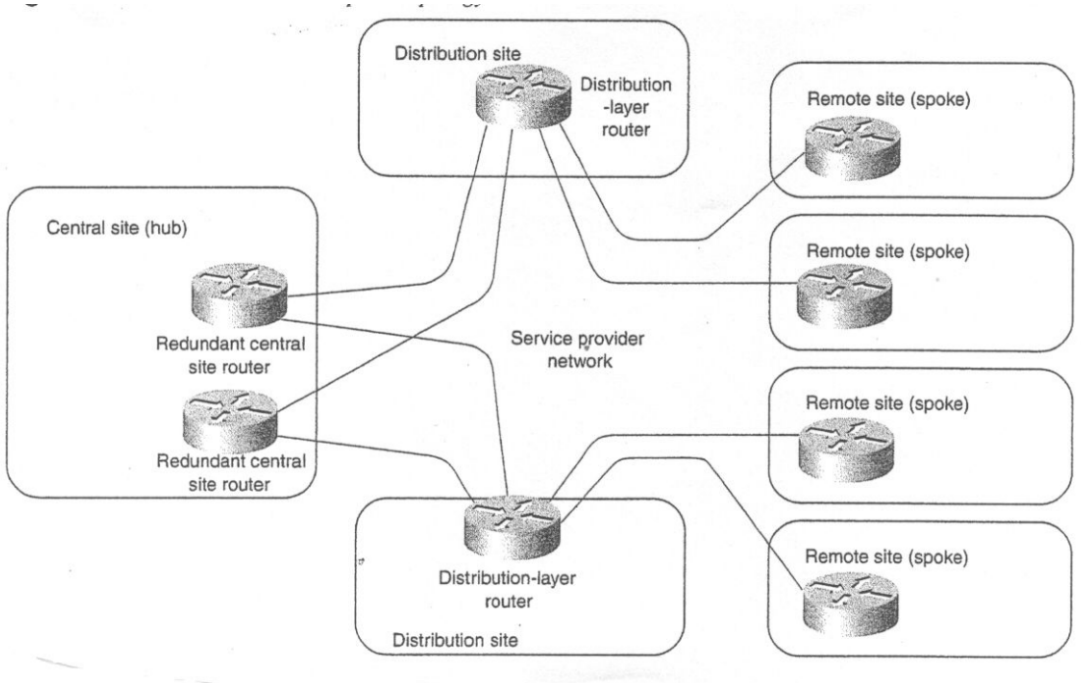
Οι επιπλέον απαιτήσεις μπορούν να περιπλέξουν παραπάνω την hub and spoke τοπολογία με την εισαγωγή dial-backup χαρακτηριστικών. Η dial-backup λύση εφαρμόζεται μέσω του δικτύου παρόχου υπηρεσίας, (για παράδειγμα μια ISDN σύνδεση φτιάχνει ένα αντίγραφο σε μια Frame Relay μισθωμένη γραμμή όπως φαίνεται στο Σχήμα 20) είναι προφανής σε ένα πελάτη αλλά δεν προσφέρει πραγματικά πλεονασμό επειδή δεν μπορεί να ανιχνεύσει πιθανές αποτυχίες(για παράδειγμα CPE ή αποτυχίες πρωτοκόλλων διακόσμησης). Ο πραγματικός end-

to-end πλεονασμός σε ένα Overlay VPN Μοντέλο μπορεί να επιτευχθεί μόνο μέσω CPE συσκευών εγκαθιστώντας μια Dial-up σύνδεση έξω από μια VPN περιοχή.



.
Σχήμα 20 Dial Backup Λύση εντός ενός δικτύου παρόχου υπηρεσίας

Συνήθως μια απλή hub and spoke τοπολογία μετατρέπεται σε μια πολυεπίπεδη τοπολογία καθώς το δίκτυο αυξάνεται. Η πολυεπίπεδη τοπολογία μπορεί να είναι μια recursive τοπολογία hub and spoke, (όμοια με το Σχήμα 21) ή μια υβριδική τοπολογία η οποία αναλύεται αργότερα σε αυτό το κεφάλαιο.



Σχήμα 21 Πολυεπίπεδη hub and spoke τοπολογία

Η hub and spoke τοπολογία που εφαρμόζεται με ένα Overlay VPN μοντέλο είναι καλά προσαρμοσμένη σε περιβάλλοντα όπου απομακρυσμένες υπηρεσίες ανταλλάσσουν δεδομένα σε μεγαλύτερη κλίμακα με τις κεντρικές τοποθεσίες παρά μεταξύ τους, καθώς τα δεδομένα ανταλλάσσονται μεταξύ των απομακρυσμένων λειτουργιών συνήθως μέσα στις κεντρικές τοποθεσίες. Αν το πλήθος των απομακρυσμένων πληροφοριών που ανταλλάσσονται αντιπροσωπεύει ένα ορισμένο μερίδιο της συνολικής κίνησης του δικτύου, η partial-mesh τοπολογία ή η full-mesh τοπολογία μπορεί να είναι πιο κατάλληλες.

5.2 Τοπολογία Πλήρους ή Μερικού πλέγματος

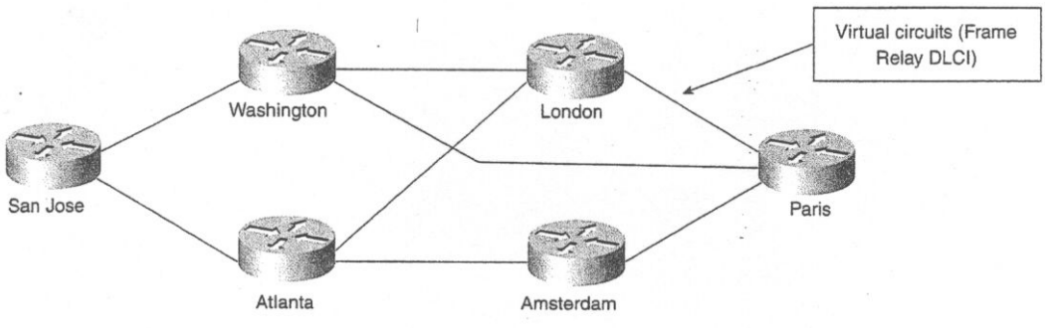
`Δεν μπορούν όλοι οι πελάτες να εφαρμόσουν τα δίκτυα τους χρησιμοποιώντας την hub-and-spoke τοπολογία για πολλούς λόγους:

1. Ο οργανισμός μπορεί να είναι λιγότερο ιεραρχικός στη δομή,απαιτώντας ανταλλαγή δεδομένων μεταξύ πολλών σημείων μέσα στον οργανισμό.

2. Το πρότυπο ανταλλαγής δεδομένων των εφαρμογών βασίζεται σε peer-to-peer επικοινωνία (συστήματα μηνυμάτων ή συστήματα επεξεργασίας).

3. Για κάποιες πολυεθνικές εταιρίες, το κόστος της hub and spoke τοπολογίας ίσως να είναι υπερβολικό εξαιτίας του υψηλού κόστους των διεθνών συνδέσεων.

Σε αυτές τις περιπτώσεις το Overlay VPN μοντέλο που θα ήταν προτιμητέο θα ήταν το μερικού πλέγματος (partial-mesh), διότι οι τοποθεσίες στα VPN που θα είναι συνδεδεμένες μέσω των VCs, θα λάμβαναν υπόψη τις απαιτήσεις κίνησης (που τελικώς θα είναι υπαγορευμένες από τις απαιτήσεις επιχείρησης). Έτσι δεν θα είναι συνδεδεμένες όλες οι τοποθεσίες με όλες τις άλλες (Σχήμα 22), αυτή η τοπολογία λέγεται partial mesh, εάν κάθε τοποθεσία έχει συνδεσιμότητα με όλες τις άλλες τοποθεσίες η τοπολογία θα λέγεται full mesh.



Σχήμα 22 Παράδειγμα ενός Partial mesh

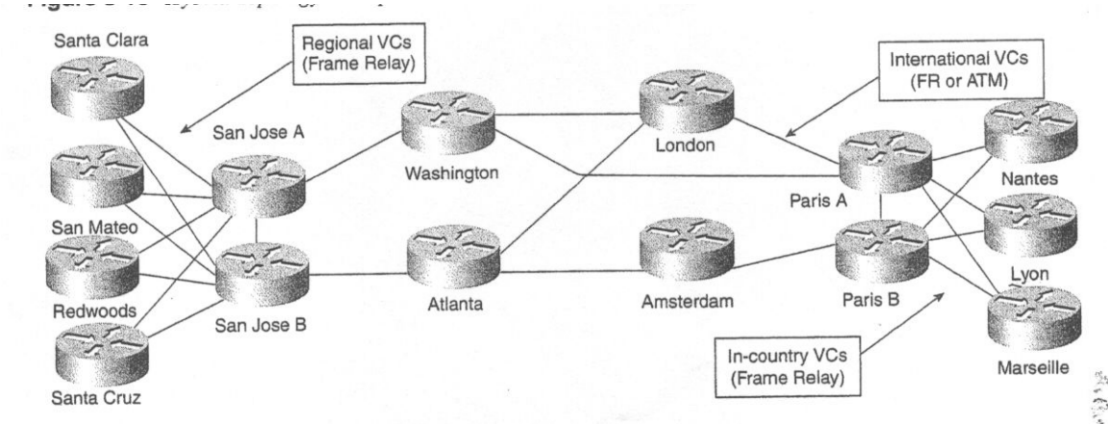
Η υλοποίηση μιας full mesh τοπολογίας είναι αρκετά απλή, το μόνο που απαιτείται είναι ένα πλέγμα (matrix) που να υποδεικνύει την κίνηση μεταξύ των σταθμών, το απαιτούμενο εύρος ζώνης μεταξύ δύο τοποθεσιών του VPN και εν συνεχεία να γίνει δέσμευση των VCs από τον πάροχο υπηρεσίας. Από την άλλη μεριά η υλοποίηση μιας partial

mesh τοπολογίας μπορεί να είναι μια πραγματική πρόκληση, καθώς πρέπει να γίνουν τα ακόλουθα:

1. Υπολογισμός της κίνησης του πλέγματος.
2. Σχεδίαση μιας partial mesh τοπολογίας βασισμένη σε μια κίνηση πλέγματος και επιπλέον λειτουργίες.
3. Καθορισμός επακριβώς πάνω σε ποίου VC την κίνηση, ανάμεσα σε δύο τοποθεσίες, η κίνηση θα αρχίσει να ρέει. Αυτό το βήμα θα πρέπει επίσης να αναμιγνύει ένα ρυθμισμένο routing protocol ότι η κίνηση ρέει πάνω στα σωστά VCs.
4. Μέτρηση του μεγέθους των VCs σε σχέση με την κίνηση του πλέγματος και το άθροισμα της κίνησης πάνω στα VCs.

5.3 Υβριδική Τοπολογία

Μεγάλα VPN χτισμένα με Overlay VPN μοντέλο τείνουν να συνδυάσουν την hub andspoke τοπολογία με την partial mesh τοπολογία. Για παράδειγμα, ένας μεγάλος πολυεθνικός οργανισμός μπορεί να έχει δίκτυα πρόσβασης σε κάθε χώρα που εφαρμόζεται μία hub and spoke τοπολογία, ενώ το κεντρικό διεθνές δίκτυο θα πρέπει να εφαρμόζεται με μια full mesh τοπολογία (Σχήμα 23).



Σχήμα 23 Παράδειγμα μιας Υβριδικής τοπολογίας

Η καλύτερη προσέγγιση στο σχεδιασμό υβριδικής τοπολογίας είναι να ακολουθηθεί ηπροσέγγιση κλασσικού ιεραρχικού σχεδιασμού δικτύου.

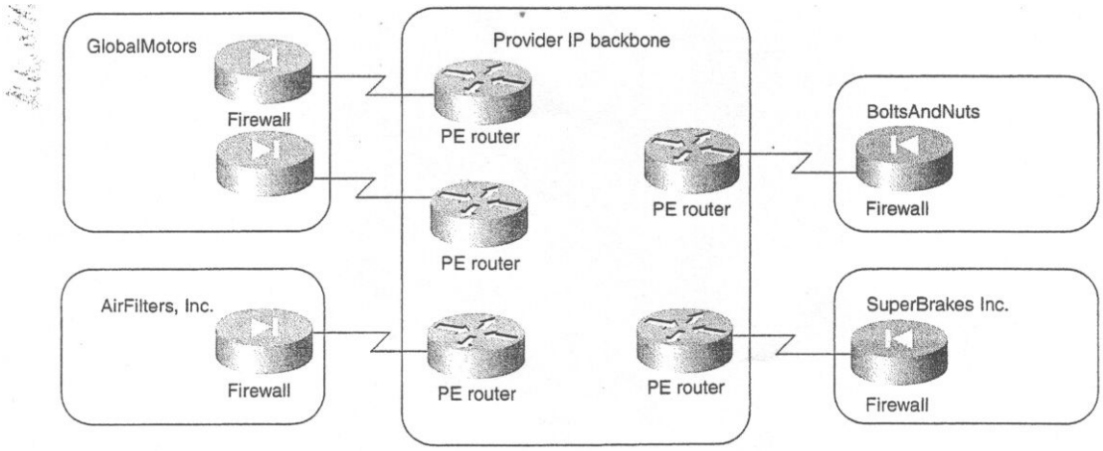
• Να διαιρεθεί το συνολικό δίκτυο σε πυρήνα, κατανεμημένα και δίκτυα πρόσβασης
• Να σχεδιαστεί ο πυρήνας και τα τμήματα πρόσβασης του δικτύου ατομικά (για παράδειγμα, Hub and spoke με dial backup στο δίκτυο πρόσβασης με το partial mesh στο κεντρικό δίκτυο
• Να συνδεθεί το κεντρικό δίκτυο και το δίκτυο πρόσβασης, μέσα από το επίπεδο διανομής με ένα τρόπο που να τα απομονώνει όσο το δυνατόν καλύτερα. Για παράδειγμα, ένα λάθος στον τοπικό βρόγχο σε ένα απομακρυσμένο γραφείο δεν θα πρέπει να αναμεταδίδεται μέσα στο κεντρικό δίκτυο. Ομοίως οι δρομολογητές του απομακρυσμένου γραφείου δεν θα πρέπει να αντιλαμβάνονται την αποτυχία ενός εκ των διεθνών συνδέσμων.

5.4 Τοπολογία Απλού Extranet

Οι Intranet τοπολογίες, που έχουν συζητηθεί ως τώρα, σχετίζονται περισσότερο με τηφυσική και τη λογική τοπολογία του VPN δικτύου, καθώς υπαγορεύονται από την VC τεχνολογία την οποία το Overlay VPN μοντέλο εφαρμόζει. Οι Extranet τοπολογίες εστιάζονται περισσότερο στις απαιτήσεις ασφαλείας του VPN δικτύου, το οποίο μπορεί να είναι εφαρμόσιμο με έναν αριθμό από διαφορετικές τεχνολογίες, είτε με το Overlay ή με το peer-topeer μοντέλο.Η παραδοσιακή extranet τοπολογία μπορεί να είναι ένα extranet που επιτρέπει σε έναν αριθμό από εταιρίες να εκτελούν any-to-any ανταλλαγή δεδομένων. Για παράδειγμα μπορεί να περιλαμβάνει εταιρίες με κοινά ενδιαφέροντα (αεροπορικές εταιρίες, κατασκευαστικές αεροπλάνων κτλ), ή μια αλυσίδα εφοδιασμού (κατασκευαστές αυτοκινήτων και όλους τους προμηθευτές τους).

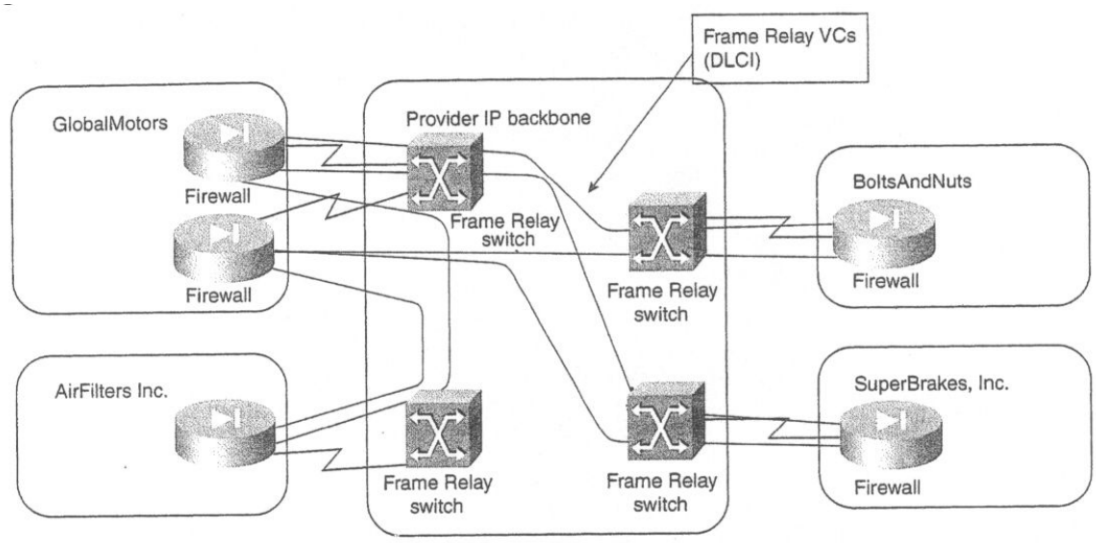
Τα δεδομένα σε ένα τέτοιο extranet μπορεί να ανταλλάσσονται μεταξύ οποιουδήποτε αριθμό από τοποθεσίες- το extranet από μόνο του δεν επιβάλει κανένα περιορισμό στην ανταλλαγή δεδομένων. Συνήθως κάθε τοποθεσία είναι υπεύθυνη για την δικιά της προστασία, φιλτράρισμα

κίνησης και firewalling. Ο μόνος λόγος χρησιμοποίησης ενός extranet αντί του κοινού Internet είναι η ποιότητα υπηρεσίας που αυτό εγγυάται και η ευαισθησία των δεδομένων που ανταλλάσσονται πάνω σε ένα τέτοιο VPN δίκτυο, το οποίο είναι ακόμα ποιο ανθεκτικό σε επιθέσεις δεδομένων από ότι το γενικό Internet. Εάν το Extranet εφαρμόζεται πάνω από ένα peer-to-peer μοντέλο (Σχήμα 24), κάθεοργανισμός καθορίζει μόνο πόσο κίνηση πρόκειται να λάβει και να στείλει από κάθε μια από τις τοποθεσίες, με αυτό τον τρόπο ο εφοδιασμός στη πλευρά του πελάτη και του παρόχου είναι πολύ απλή και αποτελεσματική η πρόσβαση.



Σχήμα 24 Παράδειγμα Extranet εφαρμοσμένο με Peer-to-Peer VPN μοντέλο

Παρόλα αυτά στο Overlay VPN μοντέλο η κίνηση μεταξύ των τοποθεσιών ανταλλάσσεται πάνω στο point-to-point VC, όμοια με το Σχήμα 25.



Σχήμα 25 Παράδειγμα Extranet εφαρμοσμένο με Overlay VPN μοντέλο

Στην extranet τοπολογία που είναι όμοια με αυτή στο Σχήμα 25, κάθε συμμετέχων οργανισμός συνήθως πληρώνει για τα VCs που χρησιμοποιεί. Φαινομενικά μόνο το απολύτως απαραίτητο VC εγκαθιδρύεται ώστε να ελαχιστοποιείται το κόστος. Ακόμα περισσότερο, οι συμμετέχοντες σε ένα τέτοιο VPN θα προσπαθήσουν να εμποδίσουν την δρομολόγηση κίνησης μεταξύ άλλων συμμετεχόντων με σκοπό να την προωθήσουν VCs που πληρώνουν οι άλλοι, συνήθως έχοντας αποτέλεσμα σε μερική μόνο συνδεσιμότητα μεταξύ των τοποθεσιών στο extranet και μερικές φορές έχοντας ακόμα σαν αποτέλεσμα σε προβλήματα στη βελτιστοποίηση της δρομολόγησης. Συνεπώς το VPN μοντέλο είναι ο προτιμότερος τρόπος εφαρμογής ενός any-to-any extranet.

5.5 Extranet Κεντρικών Υπηρεσιών

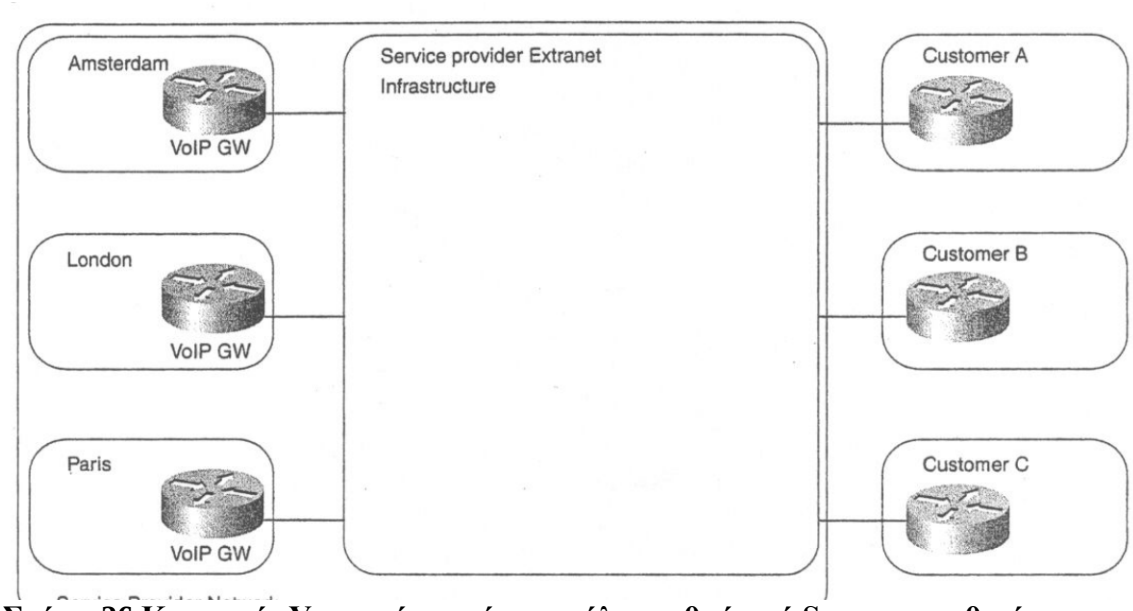
Οι οργανισμοί που σχετίζονται με συνδεσμολογία extranet και που ανήκουν στην ίδια ομάδα ενδιαφέροντος, είναι συχνά αρκετά ανοιχτοί, επιτρέποντας any-to-any συνδεσιμότητα μεταξύ των οργανισμών. Τα extranets επιτελούν ένα σκοπό (για παράδειγμα, ένα δίκτυο διαχείρισης αλυσίδας εφοδιασμού συνδέει έναν οργανισμό με όλους τους προμηθευτές του) και τείνουν να είναι περισσότερο κεντρικοποιημένα και επιτρέπουν την επικοινωνία μεταξύ των οργανισμών, χρήζοντας το extranet και όλους τους άλλους συμμετέχοντες .Άλλα παραδείγματα ενός τέτοιου extranet περιλαμβάνουν δίκτυα χρηματιστηριακώνσυναλλαγών, όπου κάθε μεσίτης μπορεί να επικοινωνήσει με το χρηματιστήριο, αλλά όχι με άλλους μεσίτες ή οικονομικά δίκτυα χτισμένα μεταξύ εμπορικών τραπεζών και της κεντρικής τράπεζας. Αν και οι σκοποί ενός τέτοιου extranet μπορούν να ποικίλουν αρκετά, όλοι μοιράζονται μια γενική ιδέα. Ένας αριθμός διαφορετικών χρηστών δέχεται πρόσβαση σε μια κεντρική υπηρεσία (που περιλαμβάνει λογισμικό, εξυπηρετητές, τοποθεσία, δίκτυο κ.λ.π.).

Η ασφάλεια στις extranet κεντρικές υπηρεσίας τυπικά εξασφαλίζεται από τον κεντρικό οργανισμό που χορηγεί το extranet. Άλλοι συμμετέχοντες με mission-critical δίκτυα (για παράδειγμα, εταιρίες χρηματιστηριακών συναλλαγών ή κεντρικές τράπεζες) ίσως επίσης να θέλουν να εφαρμόσουν τα δικά τους μέτρα ασφαλείας (για παράδειγμα, ένα firewall μεταξύ των internal δικτύων τους και του extranet).Όμοια με κάθε άλλο VPN δίκτυο, οι extranet κεντρικές υπηρεσίες μπορεί να είναι εφαρμοσμένες είτε με peer-to-peer ή Overlay VPN μοντέλο. Σε αυτή την περίπτωση, παρόλα αυτά, το peer-to-peer μοντέλο έχει αναμφισβήτητα μειονεκτήματα, επειδή ο πάροχος υπηρεσίας πρέπει να προσέχει αρκετά ότι οι συμμετέχοντες του extranet δεν μπορούν να φτάσουν ο ένας στον άλλο.

Η υλοποίηση των κεντρικών υπηρεσιών extranet από ένα VPN μοντέλο, αντιθέτως, είναι πολύ απλή και ακολουθεί τα παρακάτω βήματα:

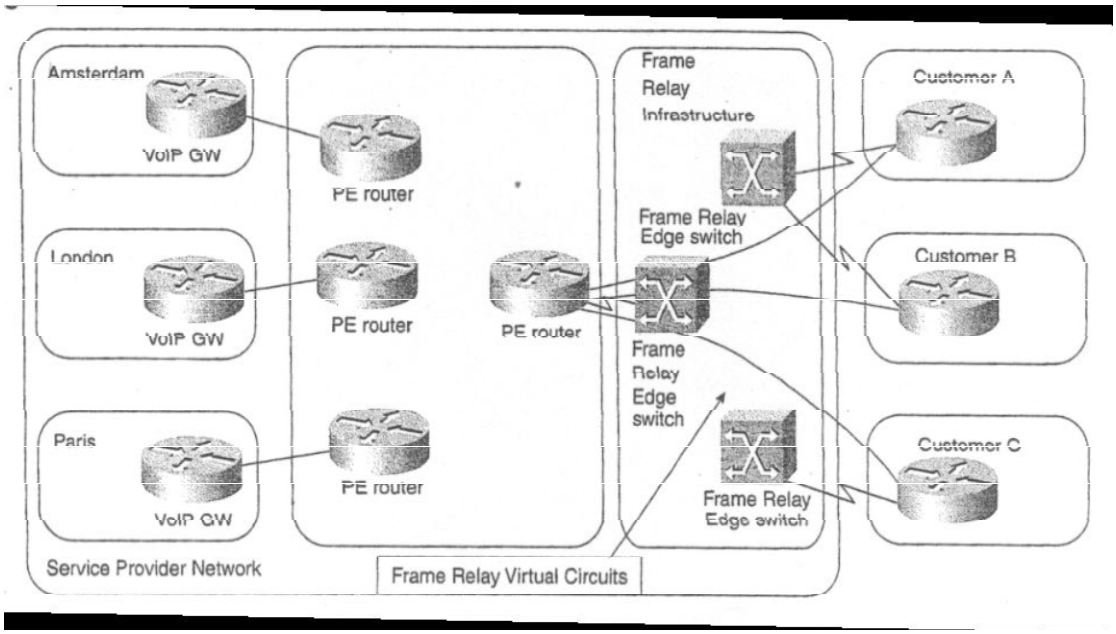
1. Παρέχονται τα VCs μεταξύ όλων των συμμετεχόντων και της κεντρικής τοποθεσίας. Το μέγεθος κάθε VC ανταποκρίνεται στις απαιτήσεις κίνησης μεταξύ του συμμετέχοντος και της κεντρικής τοποθεσίας.
2. Η κεντρική τοποθεσία ανακοινώνει τα υποδίκτυα που είναι διαθέσιμα μόνο στην κεντρική τοποθεσία στους υπόλοιπους συμμετέχοντες
3. Η κεντρική τοποθεσία φιλτράρει την κίνηση που προέρχεται από άλλους συμμετέχοντες ώστε να σιγουρέψει πως δεν θα υπάρξει πρόβλημα δρομολόγησηςς ή σκόπιμη theft-ofservice επίθεση η οποία θα επηρεάσει την σταθερότητα του VPN.

Ακολουθώντας τα τρία παραπάνω βήματα, το VPN δίκτυο του σχήματος Σχήμα 26
μετατρέπεται σε μια VC τοπολογία στο Σχήμα 25.
Μια ελάχιστα περισσότερο πολύπλοκη τοπολογία extranet κεντρικών υπηρεσιών, ίσως να περιλαμβάνει έναν αριθμό από servers διασκορπισμένους κατά μήκος αρκετών τοποθεσιών και ένας αριθμός από τοποθεσίες πελάτη έχουν πρόσβαση σε αυτούς τους servers, όμοια με το setup στο Σχήμα 26. Τυπικά παραδείγματα που θα απαιτούσαν αυτή την τοπολογία, εκφράζονται πάνω στα IP δίκτυα, όπου ένας αριθμός από χρήστες έχουν πρόσβαση σε κοινές πύλες, σε διαφορετικές πόλεις ή χώρες.



Σχήμα 26 Κεντρικές Υπηρεσίες με ένα μεγάλο αριθμό από Server τοποθεσίες

Ένα τέτοιο extranet μπορεί επίσης να υλοποιηθεί είτε με peer-to-peer μοντέλο ή με Overlay VPN μοντέλο. Ο αριθμός των VCs που απαιτείται στο Overlay VPN μοντέλο και η αντίστοιχη δημιουργούμενη πολυπλοκότητα συνήθως αποτρέπει από την υιοθέτηση του Overlay VPN μοντέλο σε αυτά τα σενάρια. Μία περισσότερο διαχειρίσιμη διαμόρφωση δικτύου θα χρησιμοποιούσε είτε ένα peer-to-peer μοντέλο είτε ένα συνδυασμό και των δύο μοντέλων, όπως απεικονίζεται στο Σχήμα 27.

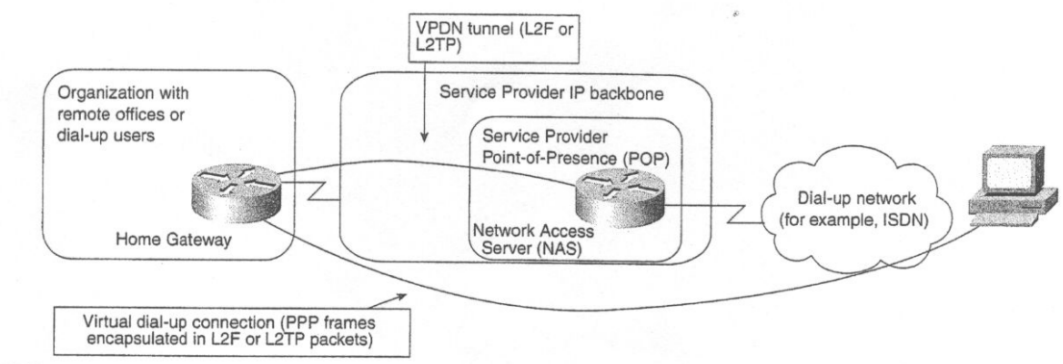


Σχήμα 27 Συνδυασμός από Peer-to-peer VPN με Overlay VPN

Λογικά, το δίκτυο στο Σχήμα 27 χρησιμοποιεί ένα peer-to-peer μοντέλο με δρομολογητή διανομής που δρουν σαν PE δρομολογητή του peer-to-peer μοντέλου. Η πραγματική φυσική τοπολογία διαφέρει από την λογική όψη: Οι δρομολογητές διανομής είναι συνδεδεμένοι με τις τοποθεσίες του πελάτη (CE δρομολογητή) μέσω του Overlay μοντέλου (για παράδειγμα το Frame Overlay Network).

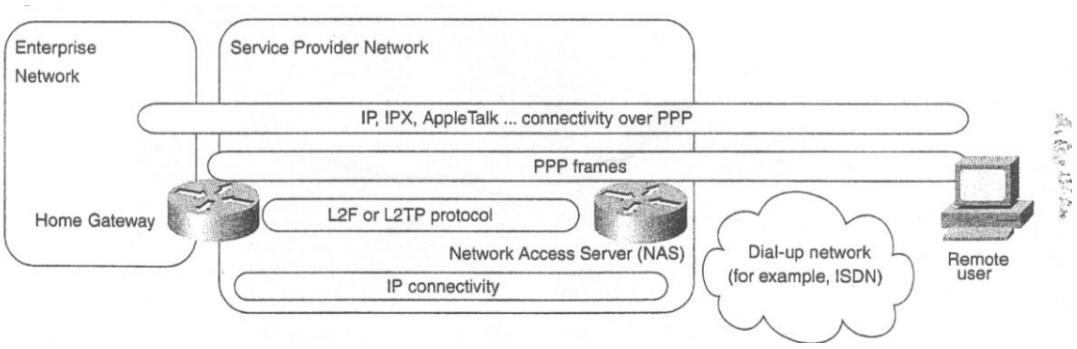
5.6 Τοπολογία VDPN

Η εικονική ιδιωτική Dial – up υπηρεσία (VPDN) (την περιγράψαμε στην προηγούμενη παράγραφο αυτού του κεφαλαίου ‘Business Problem – based VPN Classification) συνήθως εφαρμόζεται ως tunneling PPP πλαίσια που ανταλλάσσονται μεταξύ του Dial – up user την home gateway του στα IP πακέτα που ανταλλάσσονται μεταξύ του network access server όπως φαίνεται στο Σχήμα 28.



Σχήμα 28 End-to-End συνδεσιμότητα σε μια VPDN λύση

Ο Dial – up χρήστης και η home gateway εγκαθιστούν IP (ή IPX, Appletalk κτλ) σύνδεσηπάνω στο tunneled PPP σύνδεσμο και ανταλλάσσουν πακέτα δεδομένων πάνω σε αυτό. Το Σχήμα 29 δείχνει λεπτομερώς το φορτίο πρωτοκόλλου που χρησιμοποιείται μεταξύ διαφόρων μερών της VPDN λύσης.



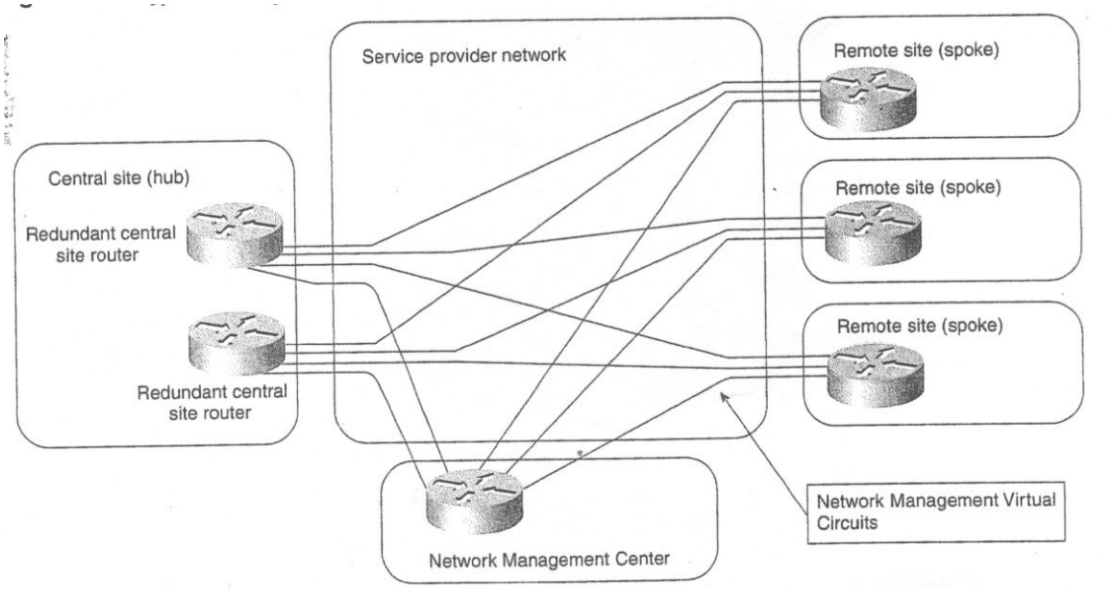
Σχήμα 29 Στοίβα Πρωτοκόλλου σε μια VPDN λύση

Κάθε VPDN λύση απαιτεί μία υποκείμενη IP υποδομή που αποτελεί τη βάση ώστε νααντταλλάσσει tunneled PPP πλαίσια μεταξύ του NAS και της home gateway. Στο απλούστερο σενάριο, το δημόσιο Internet μπορεί να χρησιμοποιηθεί ως η απαραίτητη υποδομή. Όταν οι απαιτήσεις ασφαλείας είναι αυστηρότερες, ένα VPN μπορεί να χρησιμοποιηθεί ώστε να ανταλλάσσει τα ενθυλακωμένα PPP πλαίσια. Η συγκεκριμένη προσέγγιση θεωρείται ιδιαίτερα πολύπλοκη από μερικούς σχεδιαστές δικτύων. Η πολυπλοκότητα αυτή όμως μπορεί να γίνει κατανοητή αν γίνει ο παρακάτω διαχωρισμός:

• Ο NAS και η home gateway χρησιμοποιούν οποιαδήποτε IP υποδομή είναι διαθέσιμη, ώστε να ανταλλάξουν τα VPDN δεδομένα, τα οποία μπορούν να θεωρηθούν σαν μία αίτηση που δεν κάνει καμία ενέργεια στην κορυφή της IP ουράς. Συνεπώς η εσωτερική δομή της υποκείμενης IP υποδομής δεν επηρεάζει την ανταλλαγή των δεδομένων της αίτησης, και τα περιεχόμενα της αίτησης (τα IP πακέτα στα ενθυλακωμένα PPP πλαίσια σε ένα VPDN φάκελο) δεν αλληλεπιδρούν με τους δρομολογητές που παρέχουν την IP υπηρεσία.
• Το υποκείμενο IP δίκτυο θεωρείται ένα extranet κεντρικών υπηρεσιών με πολλές τοποθεσίες εξυπηρετητών (NES), και μία home gateway η οποία δρα σαν τοποθεσία πελάτης. Αυτή η υποδομή μπορεί να υλοποιηθεί με μια σειρά από τρόπους, από το αμιγώς Overlay VPN μοντέλο ως το αμιγώς peer–to–peer μοντέλο.

5.7 Τοπολογία Διαχειριζόμενου Δικτύου VPN

Η τελευταία VPN τοπολογία που αναλύεται σε αυτό το κεφάλαιο, είναι η τοπολογία που χρησιμοποιείται από τους παρόχους υπηρεσίας ώστε να διαχειρίζονται αποτελεσματικά τους δρομολογητές των πελατών τους μέσω σαφώς ορισμένων υπηρεσιών διαχείρισης δικτύου. Σε μια τυπική διαμόρφωση, που φαίνεται στο Σχήμα 30 ο πάροχος υπηρεσίας προμηθεύει έναν αριθμό από δρομολογητές, συνδέοντας αυτούς μέσω των VCs που εφαρμόζονται με ATM η Frame Relay και χτίζει μία διαχωρισμένη hub-and-spoke τοπολογία συνδέοντας κάθε πελάτη – δρομολογητή με το NMC (Network Management Center).



Σχήμα 30 Τυπική τοπολογία δικτύου διεύθυνσης

Η VPN τοπολογία που χρησιμοποιείται στο τμήμα πελάτης του δικτύου μπορεί να είναι κάθε τοπολογία που υποστηρίζεται με το VPN μοντέλο που αποτελεί την κύρια βάση, που κυμαίνεται από την hub-and-spoke στη full mesh τοπολογία. Η τοπολογία που χρησιμοποιείται στο CPE μέρος διεύθυνσης του δικτύου, αποτελεσματικά θα μπορούσε να ήταν μία κεντρική extranet υπηρεσιών τοπολογία με τους δρομολογητές πελάτες να λειτουργούν σαν πελάτες και το Κέντρο `ιαχείρισης `ικτύων (Network Management Center) να γίνεται η κεντρική τοποθεσία του extranet διεύθυνσης.Όπως εξηγήθηκε στην παράγραφο Central – services – Extranet νωρίτερα σε αυτό το κεφάλαιο- τέτοια τοπολογία είναι ευκολότερο να υλοποιηθεί με μία hub-and-spoke τοπολογία του Overlay VPN μοντέλου, το οποίο επίσης εξηγεί γιατί οι περισσότεροι διαχειριστές δικτύων των παρόχων υπηρεσιών χρησιμοποιούν το setup του Σχήμα 30.

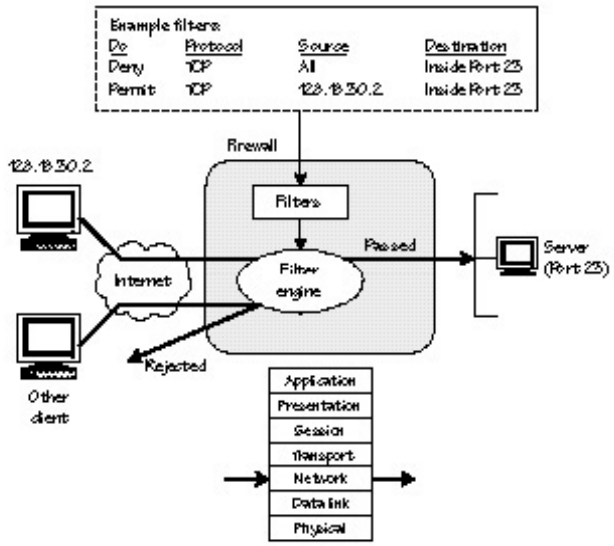
6. «Τοίχοι ασφαλείας» (Firewalls)

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)

6.1 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 31, επιτρέπεται η είσοδος μόνο σε πακέτα που προέρχονται από υπολογιστή με IP διεύθυνση 128.18.30.2.



Σχήμα 31: 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.

6.2 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 . 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.

6.2.1 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.

6.2.2Application 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.

6.3 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.

7. Η ΠΥΛΗ VPN

Μια πύλη VPN, που ονομάζεται επίσης και ένα VPN router, είναι μια σχέση που συνδέει το σημείο δυο LANs το οποίο είναι συνδεδεμένο με μια ασφαλή δίκτυο όπως το Internet. Μια πύλη VPN, επομένως, είτε συνδέεται με μια ενιαία πύλη VPN, ή σε πολλαπλές πύλες VPN για την επέκταση του LAN. Αυτό το σενάριο είναι συνήθως αναφέρεται ως δρομολογητής -to-router VPN. Τα εταιρικά δίκτυα που συνδέονται μεταξύ τους μέσω της VPN servers τρέχουν δρομολόγησης και απομακρυσμένης πρόσβασης (RRAS). Το πραγματικό μέσο που συνδέει το LANs είναι συνήθως το Διαδίκτυο. Αυτό σημαίνει ότι η πύλη VPN ή δρομολογητή θα ρυθμιστεί με τη διεύθυνση στο LAN που είναι συνδεδεμένοι και μια δημόσια διεύθυνση IP.

Λίγοι παράγοντες που επηρεάζουν το σχεδιασμό και την υλοποίηση του VPN πύλες είναι:

- Εκχώρηση διεύθυνσης IP
- Όνομα ψήφισμα
- Δυναμικές δρομολόγηση
- Auto-στατική δρομολόγηση ενημερώσεις
- Συντήρηση του πίνακα δρομολόγησης

Πελάτες μπορούν να λάβουν διευθύνσεις IP και ονομάτων διακομιστή πληροφορίες από το διακομιστή VPN ή να μπορούν οι πληροφορίες από ένα VPN server εκπλήρωση του ρόλου του DHCP Relay Agent.

Οι περισσότερες πύλες VPN έχουν *κομβικού και ακτινωτού Configuration design.* Το πλεονέκτημα αυτής της ρύθμισης του σχεδιασμού είναι ότι το εταιρικό δίκτυο μπορεί να διαχειριστεί την πρόσβαση στο Internet. Ένα άλλο πλεονέκτημα του *κομβικού και ακτινωτού διαμόρφωση του σχεδιασμού* είναι ότι ένα μη πολύπλοκο δίκτυο δρομολόγησης ρύθμιση μπορεί να χρησιμοποιηθεί.

Ένα σημαντικό στοιχείο των πύλων VPN δικτύων είναι *η επίλυση ονομάτων.* Αυτό οφείλεται σε πελάτες που χρειάζονται για να διερευνούν την κατάλληλη επίλυση ονομάτων διακομιστών για τον εντοπισμό τόσο των τοπικών πόρων και των απομακρυσμένων πόρων. Ο DHCP server θα πρέπει να παρέχει τις διευθύνσεις IP των εν λόγω ονομάτων διακομιστών για την πύλη VPN δίκτυα να λειτουργούν. WINS ή διακομιστές DNS μπορεί να παρέχει υπηρεσίες επίλυσης ονομάτων. Αυτοί οι διακομιστές ονομάτων μπορεί να είναι επί του τοπικού LAN, ή πελάτες μπορούν να χρησιμοποιούν την σύνδεση VPN για να προωθήσει τα αιτήματά τους να έχουν πρόσβαση σε πόρους για την εξ αποστάσεως πρόσβαση σε διακομιστές. Με το DNS, το όνομα ψηφίσματος μπορούν επίσης να παρέχονται από το Internet DNS servers.

Πρωτόκολλα δρομολόγησης δρομολογητές επιτρέπουν να επικοινωνούν μεταξύ τους, και να διαφημίσουν διαθέσιμα δρομολόγια και τις συνδεδεμένες με προτίμηση στους άλλους δρομολογητές στο

δίκτυο. Τα πρωτόκολλα δρομολόγησης που μπορείτε να προσθέσετε όταν χρησιμοποιεί την υπηρεσία δρομολόγησης και απομακρυσμένης πρόσβασης (RRAS) στα Windows Server 2003 είναι:

- Η Routing Information Protocol (RIP) πρωτόκολλο δυναμικής δρομολόγησης
- Το Open Shortest Path First (OSPF) πρωτόκολλο δυναμικής δρομολόγησης
- Το πρωτόκολλο δρομολόγησης multicast IGMP Router και proxy
- Το DHCP Relay Agent

Χρησιμοποιώντας *δυναμικά πρωτόκολλα δρομολόγησης,* όπως το RIP και OSPF προσθέτει το πλεονέκτημα της απλοποιημένης διαχείρισης, επειδή το μερίδιο επικαιροποίηση των πληροφοριών δρομολόγησης μεταξύ των δρομολογητών, και επίσης διαχειρίζεται τον πίνακα δρομολόγησης ώστε να περιέχει τρέχουσες, ενημερωμένες πληροφορίες. Όταν δρομολογητές πρέπει να διαβιβάσει τα πακέτα, θα ερμηνεύσει τις διευθύνσεις των πακέτων, και στη συνέχεια να χρησιμοποιήσουν τις πληροφορίες σε πίνακες δρομολόγησης να περάσει το πακέτο. Πακέτων δεδομένων περιέχει τόσο προέλευσης και προορισμού τις διευθύνσεις τους στο κεφαλίδων πακέτων. Αυτή είναι η πληροφορία που χρησιμοποιείται κατά τη δρομολόγηση των αποφάσεων πρέπει να γίνουν. Η διεύθυνση προορισμού συγκρίνεται με την τοπική διεύθυνση για να διαπιστωθεί κατά πόσον το πακέτο θα πρέπει να αποσταλούν μέχρι τη στοίβα με τις τοπικές υποδοχής, αν το πακέτο θα πρέπει να σταλεί σε έναν διαφορετικό προορισμό, ή αν το πακέτο θα πρέπει απλά να αγνοηθεί.

OSPF είναι η δυναμική δρομολόγηση πρωτόκολλο που χρησιμοποιείται για την ανταλλαγή πληροφοριών δρομολόγησης σε μεγάλες έως πολύ μεγάλων δικτύων. Ενώ η ρύθμιση OSPF είναι πιο περίπλοκη από ό, τι είναι να ρυθμίσετε και να διαχειρίζονται τα ΠΕΠ, OSPF είναι αποτελεσματικότερη από την ΠΕΕ, και απαιτεί επίσης πολύ μικρό δίκτυο γενικά. Λίγες λόγους να χρησιμοποιήσει OSPF αντί ΠΕΕ οφείλεται σε OSPF κλιμάκωση καλά σε μεγάλες και πολύ μεγάλες internetworks, OSPF hop δεν έχει κανένα όριο, OSPF υπολογίζονται οι διαδρομές είναι η loop-δωρεάν δρομολόγια, και OSPF χρησιμοποιεί λιγότερο εύρος ζώνης δικτύου από το πρωτόκολλο δρομολόγησης RIP.

Δρομολογητές RIP ότι έχουν ενεργοποιηθεί? Διαφημίσετε το σύνολο του περιεχομένου τους στους πίνακες δρομολόγησης σε άλλους τους δρομολογητές, σε 30 δεύτερα διαστήματα. Από αυτό, είναι απολύτως σαφές ότι η ΠΕΕ επιβαρύνονται με ένα αρκετά μεγάλο ποσό της κυκλοφορίας στο δίκτυο.
Αυτό θα μπορούσε να επηρεάσει αρνητικά τις συνδέσεις dial-up ζήτησης λόγω της ποσότητας των ΠΕΕ κυκλοφορίας που θα προκύψει.
Η Auto-στατική δρομολόγηση ενημερώσεις μπορεί να χρησιμοποιηθεί για τα δίκτυα που χρησιμοποιούν ΠΕΕ. Με auto-στατική δρομολόγηση ενημερώσεις, οδός ενημέρωση διαφημίσεις μπορεί να προγραμματιστεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1)Σημειώσεις «Σχεδίαση Εικονικών Δικτύων» ΤΕΙ Λαμίας του Καθηγητή Οδυσσέα Ι. Πυροβολάκη.

2)Σημειώσεις ΣΧΕΔΙΑΣΗ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ ΤΕΙ Λαμίας του
Καθηγητή Κωνσταντίνου Λιμνιώτη.

3)Περιοδικό OTE chat ΙΑΝΟΥΑΡΙΟΣ 2008 No 1

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ

Dave Kosiur, “Building and Managing Virtual Private Networks”, John Wiley & Sons, 1998.

Gordon Chaffee , “Διαλέξεις από το Πανεπιστήμιο του Berkeley” (2005)

Charlie Scott, Paul Wolfe and Mike Erwin, “Virtual Private Networks – Second Edition”, O’Reilly, 1999.

ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

http://www.tech-faq.com/lang/el/vpn-gateway.shtml&usg=ALkJrhinP1WbTZoaBrOb7TDEzRhL7djgXQ