ABSTRACT

The term "virtual private networks" is being used the last few years by service providers and private companies. However, each of these private companies, define the "virtual private networks" in a way suitable for company's needs and according to the services provide to market. Generaly speaking we could define "virtual private networks" as the local or wide area networks of a company which uses the PSTN (Public Switched Telephone network) as the main carrier of communications instead of private dedicated lines (leased-lines).

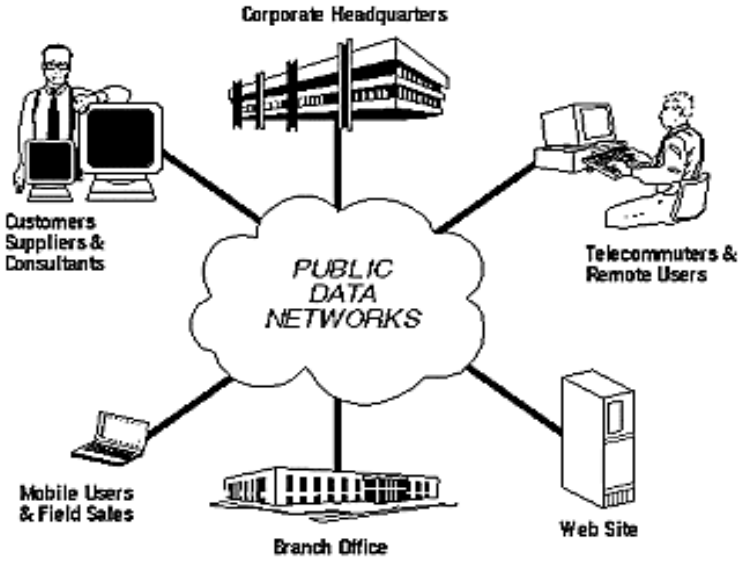
ΠΕΡΙΛΗΨΗ

Ο όρος ¨Εικονικά Ιδιωτικά Δίκτυα¨ (Virtual Private Networks) άρχισε να αναφέρεται πάρα πολύ , μόλις τα τελευταία χρόνια . Κάθε εταιρία δίνει το δικό της χαρακτηρισμό ανάλογα με το πώς τα αντιλαμβάνεται και βεβαίως τι προσφέρει η ίδια στην αγορά. Γενικά όμως θα μπορούσαμε να ορίσουμε σαν Virtual Private Networks (VPNs) τα εσωτερικά ή εξωτερικά δίκτυα εταιριών (Intranets και Extranets) τα οποία χρησιμοποιούν το δημόσιο δίκτυο (Public Switched Telephone Network) ως κύριο μέσο επικοινωνίας , αντί αφιερωμένων ιδιωτικών γραμμών(eased Lines) για την μεταφορά στοιχείων.

ΠΡΟΛΟΓΟΣ

Το Internet αποτελεί αναμφισβήτητα ένα από τα μεγαλύτερα τεχνολογικά επιτεύγματα του αιώνα. Ξεκινώντας ως ένα απλό δίκτυο που συνέδεε υπολογιστές κρατικών Υπηρεσιών ή Πανεπιστημίων στις Ηνωμένες Πολιτείες τώρα πλέον είναι το μεγαλύτερο δίκτυο πληροφοριών,διασκέδασης και επικοινωνίας του πλανήτη.Τα τελευταία χρόνια εξελίσσεται και μεταλλάσσεται σε χώρο εμπορικής δραστηριότητας με τους δικούς του νόμους ,περιορισμούς και προϋποθέσεις .

Το Internet στο χώρο αυτό επεκτείνεται σε δύο κυρίως επίπεδα: το δημόσιο (public level) και το ιδιωτικό (private level).Το πρώτο είναι εδώ και χρόνια σε ανάπτυξη και αφορά κυρίως εφαρμογές ηλεκτρονικού εμπορίου (e-commerce) δηλ. την παροχή υπηρεσιών ή την πώληση αγαθών .Το δεύτερο αναπτύσσεται ραγδαία τελευταίως και έχει να κάνει με τη χρήση του Διαδικτύου από μεγάλες επιχειρήσεις σαν μέσο μετάδοσης των στοιχείων και πληροφοριών τους (data) που είναι απαραίτητο να μεταφερθούν γρήγορα , σίγουρα και χωρίς υποκλοπές.



Εικόνα 1.Το Internet στο χώρο των επιχειρήσεων

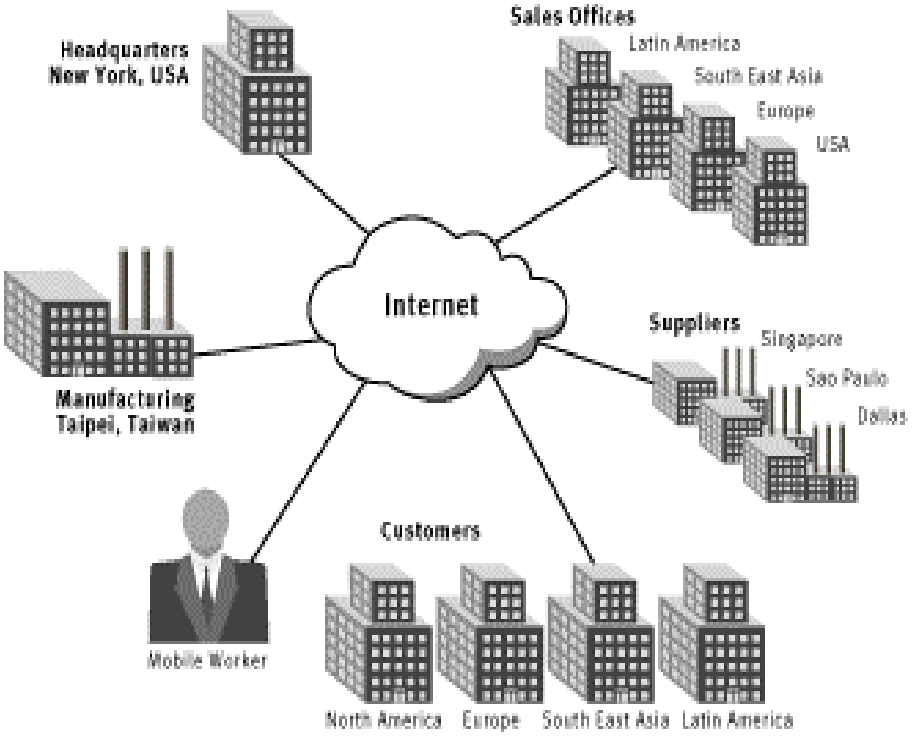
2 . ΚΥΡΙΑ ΣΗΜΕΙΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΩΝ VPNS

Η παγκοσμιοποίηση της αγοράς και η εξέλιξη της τεχνολογίας ανάγκασε πολλές επιχειρήσεις να αλλάξουν τον τρόπο εργασίας τους.Οι επιχειρήσεις αυτές πρέπει πλέον να διατηρούν υποκαταστήματα σε πολλά μέρη του κόσμου,να έχουν εργαζόμενους που ταξιδεύουν ,να μοιράζουν στοιχεία τους σε πελάτες και προμηθευτές .Για να γίνει αυτό μέχρι τώρα χρησιμοποιούταν ευθείες γραμμές (leased lines) συνδέοντας το σημείο επαφής με το κεντρικά καταστήματα-γραφεία με τοπολογία "αστέρα". Έτσι το κόστος για τη συντήρηση τέτοιων γραμμών ήταν υπερβολικά υψηλό, το δίκτυο φορτωνόταν πάρα πολύ και επίσης το πρόβλημα της αποκοπής και μη λειτουργίας των υποκαταστημάτων αν κάτι συνέβαινε στα κεντρικά ,πάντα υπήρχε.

Αντί λοιπόν της χρήσης τέτοιων γραμμών τα Internet-based VPNs χρησιμοποιούν τη βασική υποδομή του Internet για τη μετάδοση των πληροφοριών και των στοιχείων (data).Τα πλεονεκτήματα τους συνοψίζονται στα εξής:

- **Χαμηλό κόστος** . Οι μισθωμένες γραμμές (leased lines) T1(1.5 Mbps) και T3 (45 Mbps) απαιτούν μεγάλο μηνιαίο πάγιο και χρέωση ανάλογα με την απόσταση των συνδεδεμένων σημείων.Οι αντίστοιχες T1 και T3 σε Frame-relay δίκτυα απαιτούν επίσης μηνιαία πάγια χρέωση καθώς και επιπλέον χρήματα για κάθε Permanent Virtual Circuit (PVC) που δημιουργείται . Αντίθετα γραμμές με τις ίδιες ταχύτητες σε τοπικό παροχέα Internet (ISP) στοιχίζουν πολύ λιγότερο ή μπορούν και να αποφθεχθούν αφού η διασύνδεση μπορεί να γίνει από παντού με μια απλή σύνδεση και όλα τα πλεονεκτήματα των ανωτέρω.
- **Ευκαμψία (Flexibility)**. Στα παραδοσιακά δίκτυα έπρεπε να υπάρχει συμβατός εξοπλισμός που να υποστηρίζει όλα τα περιφερειακά γραφεία ή τους απομακρυσμένους κλάδους της επιχειρήσεις . Στα VPN's δεν υπάρχει περιορισμός ή προβλήματα ασυμβατότητας εξοπλισμού αφού απλά και μόνο η σύνδεση με έναν ISP αρκεί για την επικοινωνία.

- **Επεκτασιμότητα (scalability)** . α) Η χρήση του Internet ως μέσο μετάδοσης προσφέρει γεωγραφική διάχυση .Πολύ εύκολα και από οποιοδήποτε μέρος του κόσμου πελάτες , προμηθευτές ή άνθρωποι της επιχείρησης συνδέονται χωρίς δυσκολία με αυτήν. β) Οι συνδέσεις αυτές είναι εύκολα αναβαθμίσιμες ανάλογα με τις απαιτήσεις χωρίς όμως και υποχρεωτική αναβάθμιση του εξοπλισμού σε κάθε σημείο (point) αφού αλλάζει μόνο το είδος της σύνδεσης με τον ISP.



Εικόνα 2. Η παγκοσμιοποίηση στο χώρο των επιχειρήσεων και η ανάγκη για VPNs.

3 . Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΝΟΣ VPN

Τα βασικά δομικά στοιχεία ενός Virtual Private Network είναι :
α) η διαδικασία γνωστή ως tunneling η δημιουργία δηλαδή "σήραγγας "για την μετάδοση "πακέτων" των data διαμέσω του Internet και
β)η ασφάλεια (security) που απαιτείται για την προστασία κατά τη μεταφορά αυτών των δεδομένων λόγω της ιδιαιτερότητας του περιβάλλοντος αυτού.

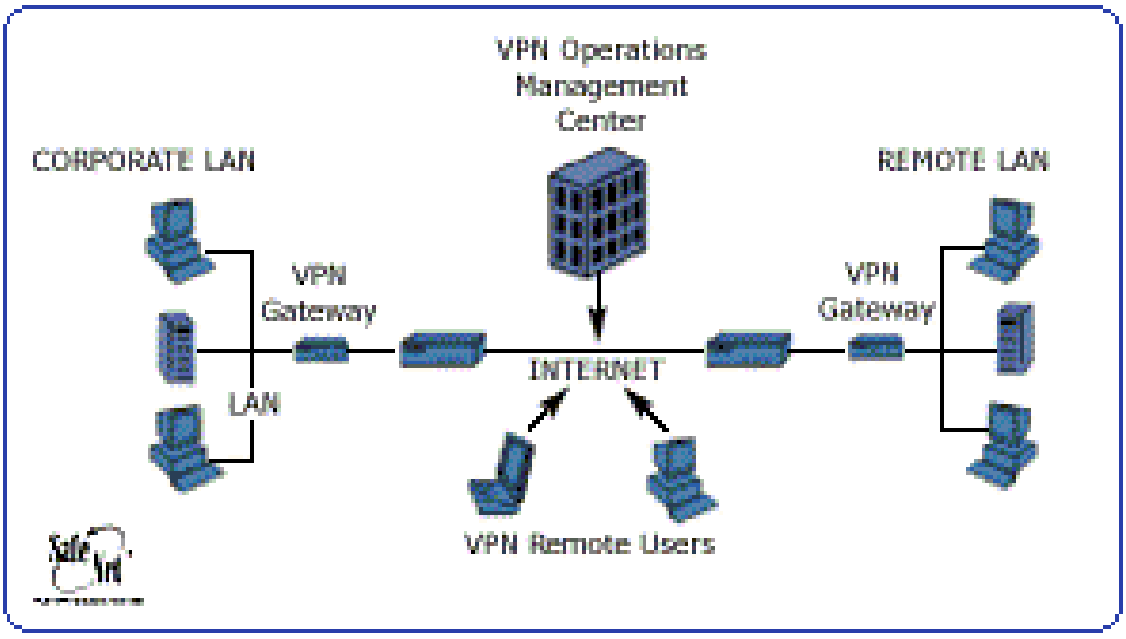
Ο όρος virtual εμπεριέχει δυναμική. Αντίθετα με τις ευθείες γραμμές όπου χρησιμοποιούνται μόνιμες συνδέσεις μεταξύ των σημείων , εδώ η σύνδεση δημιουργείται μόνο για το χρόνο που απαιτείται για την εκτέλεση της εργασίας και κατόπιν διακόπτεται αφήνοντας το δίκτυο και τον εξοπλισμό ελεύθερο για άλλη χρήση . Επίσης ο όρος σημαίνει λογική και όχι φυσική δομή όπως για παράδειγμα στα LAN's. Το δίκτυο υφίσταται ,μεταβάλλεται, τροποποιείται ανάλογα με το σημείο και το χρόνο που γίνεται η σύνδεση χρησιμοποιώντας εξωτερικό εξοπλισμό (του ISP) και όχι κατ'ανάγκη της ίδιας της εταιρίας.

Το "tunneling" είναι το κυριότερο χαρακτηριστικό των VPN's. Η τεχνική έχει περίπου ως εξής :Δημιουργείται μια ειδική σύνδεση μεταξύ δύο σημείων (endpoints). Με ειδικό software στον αποστολέα ενσωματώνονται (encapsulation) τα IP πακέτα σε άλλα και έτσι ταξιδεύουν μέσω Internet .Τα μεγαλύτερα αυτά πακέτα έχουν νέο IP header και κρυπτογράφηση. Κατά τη στιγμή που ο παραλήπτης τα δέχεται , αφαιρείται , γίνεται η αποκρυπτογράφηση και παραδίδεται το αρχικό πακέτο.

Η ασφάλεια είναι το δεύτερο σημαντικό κομμάτι των VPN's.Ο όρος "Private"σημαίνει ότι δημιουργείται μια "προσωπική-ιδιωτική" σύνδεση μεταξύ δύο σημείων παρ' όλο που χρησιμοποιείται το κοινό τηλεφωνικό δίκτυο ή που συνταξιδεύουν παράλληλα και άλλα δεδομένα . Επίσης σημαίνει ασφάλεια και προστασία από κάθε λογής υποκλοπή αφού όλα τα δεδομένα θεωρούνται σημαντικά και απόρρητα .Πρέπει δηλαδή να διασφαλίζονται τα εξής σημαντικά :

- **Πιστοποίηση** ότι τα δεδομένα έρχονται από την πηγή που διατείνονται,
- **Πρόσβαση** μόνο σε εξουσιοδοτημένους χρήστες ,
- **Εμπιστοσύνη** ότι κανείς δε διαβάζει ή αντιγράφει στοιχεία και
- **Ακεραιότητα** και μη αλλοίωση των data κατά τη μεταφορά τους .

Υπηρεσίες ασφάλειας προσφέρονται πλέον σε όλα τα επίπεδα του μοντέλου OSI όπως στα ανώτερα application και session καθώς επίσης στα κατώτερα network και data-link.



Εικόνα 3.Τα VPNs over Internet

3.1.TUNNELING ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ

Υπάρχουν δύο κύριες αρχιτεκτονικές στη διαδικασία "tunneling": Η "client-initiated" και η "client-transparent".Η πρώτη απαιτεί ειδικό software και από τα δύο σημεία επικοινωνίας τον client και τον server (ή gateway).Ο client ανοίγει το tunnel το οποίο και τερματίζεται στην πλευρά της επιχείρησης .Ο ISP δεν μετέχει στο tunneling.Χρησιμοποιείται πιστοποίηση (authentication) με ID's και passwords ή με άλλου είδους ψηφιακές υπογραφές .Από τη στιγμή όμως που δημιουργείται το tunnel ο Internet Service Provider είναι σα να μην υπάρχει καθόλου.

Στη δεύτερη περίπτωση -την client-transparent- ο ISP πρέπει να έχει ειδικούς servers ή routers που να υποστηρίζουν ειδικά πρωτόκολλα tunneling.Η διαδικασία έχει ως εξής: Ο client συνδέεται με τον ISP δηλώνοντας ότι επιθυμεί να συνδεθεί με συγκεκριμένη τοποθεσία και με ειδική σύνδεση δηλ.tunneling (αυτό μπορεί να γίνει και αυτόματα βάση στοιχείων που εμπεριέχονται στο user-ID) .Ο access server στη συνέχεια εγκαθιστά σύνοδο (session) με τον tunnel server στην επιχείρηση. Εδώ υπάρχει το πλεονέκτημα ότι δεν είναι απαραίτητο ο client να έχει ειδικό software εγκατεστημένο.

Παρ΄όλο που η τεχνολογία VPN είναι σχετικά καινούργια υπάρχουν ήδη αρκετά πρωτόκολλα που λειτουργούν κυρίως στο δεύτερο, τρίτο και πέμπτο επίπεδο του μοντέλου OSI. Επίσης παρ΄όλο που χωρίζονται σε πρωτόκολλα που ασχολούνται με το tunneling και την ασφάλεια και σε πρωτόκολλα που ασχολούνται με τη διαχείριση του δικτύου η διάκριση αυτή δεν είναι απόλυτη καθότι στη διαχείριση εμπλέκονται διαδικασίες κρυπτογράφησης και authentication.

A/A	PROTOCOL	JOB	OSI LAYER	TYPE of VPN
1	PPTP	Tunneling/Security	Layer 2	Basic remote access
2	L2F	Tunneling/Security	Layer 2	
3	L2TP	Tunneling/Security	Layer 2	Basic remote access
4	IPSec	Tunneling /Security/Management	Layer 3	Trusted LAN to LAN
5	Socks v5	Tunneling/Security	Layer 5,7	Secure remote access
6	RADIUS	Management		
7	ISAKMP	Management		

Πίνακας 1.Τα πρωτόκολλα αναφορικά με την υπηρεσία που προσφέρουν

3.1.1. IPSEC PROTOCOL

Θεωρείται το πιο πλήρες πρωτόκολλλο αφού τα άλλα (PPTPκαι L2TP) χρησιμοποιούν μέρη από το το IPSec, αλλά επίσης γιατί έχει εφαρμογή σε LAN-to-LAN και client-to-LAN δίκτυα .

Η ανάπτυξή του ξεκίνησε γιατί διαπιστώθηκε αδυναμία των TCP/IP στον τομέα της ασφάλειας που όμως είναι πολύ σημαντική μιας και το Inter-net πλέον βρίθει εμπορικών εφαρμογών. Βασίζεται σε μελέτες σύμφωνα με τα RFCs 1825 και 1829 που δημοσιεύτηκαν μόλις το 1995 από την IETF (Internet Engineering Task Force). Το IP packet είναι το βασικό συστατικό στα IP δίκτυα γιατί περιλαμβάνει πληροφορίες για την πηγή, τον προορισμό και το είδος των data που μεταφέρει. Το IPSec ορίζει δύο νέα headers σε κάθε IP πακέτο :Ένα για πιστοποίηση (Authentication Header-AH)και ένα για ενθυλάκωση (Encapsulating Security Payload-ESP).

Το IPSec χρησιμοποιεί έναν αριθμό από τεχνολογίες κρυπτογράφησης και πιστοποίησης όπως :

- Το κλειδί Diffie-Hellman για ανταλλαγή μεταξύ δύο σημείων
- Το δημόσιο κλειδί Diffie-Hellman

- Data Encryption Standard (DES)
- Ψηφιακή πιστοποίηση για δημόσια κλειδιά
- Διάφορους Hash αλγόριθμους.

Τρία όμως είναι τα βασικά συστατικά του:

α)Security Association(SA).Για να γίνει δυνατή μια ασφαλής ανταλλαγή δεδομένων μεταξύ δύο πλευρών πρέπει να προσυμφωνηθούν οι κρυπτογραφικοί αλγόριθμοι που θα χρησιμοποιήσουν ο τρόπος και η συχνότητα ανταλλαγής κλειδιών κ.λ.π. Πιο συγκεκριμένα καθορίζονται τα εξής:

- Ο τρόπος που χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης(encryption) στο Encaptulating Security Payload (ESP) και τα κλειδιά του.
- Το είδος των αλγόριθμων και τα κλειδιά που χρησιμοποιούνται για πιστοποίηση και κρυπτογράφηση
- Η συχνότητα ανταλλαγής και τροποποίησης των κλειδιών αυτών
- Ο χρόνος ζωής τους
- Ο χρόνος ζωής ολόκληρου του SA
- Ο τρόπος που χρησιμοποιείται ο αλγόριθμος πιστοποίησης(authentication) στο Authentication Header (AH) και τα κλειδιά του.
- Η παρουσία και το μέγεθος κάθε άλλου τρόπου κρυπτογράφησης που χρησιμοποιείται μαζί με τον αλγόριθμο

Το SA μπορούμε να το φανταστούμε σαν ένα είδος σύμβασης μεταξύ δύο μελών για τη μεταξύ τους ανταλλαγή data.Σε περιπτώσεις που μία επιχείρηση με δικό της VPN συνδέεται με μία άλλη που επίσης έχει VPN με το SA καθορίζεται ποιος έχει πρόσβαση σε ποιους πόρους του δικτύου .Επίσης υπάρχουν διαφορετικά sets SA για τους υπαλλήλους τους πωλητές ή ακόμα ακόμα για διαφορετικά τμήματα της επιχείρησης. Για επιπρόσθετη ασφάλεια, κάθε Security Association(SA) δεν ισχύει για αμφίδρομη επικοινωνία αλλά για μια κατεύθυνση αποστολέα-παραλήπτη .Για να συμβεί και το αντίστροφο πρέπει να συμφωνηθεί ακόμα ένα SA.

β)Authentication Header (AH).Σχεδιάστηκε για να εξυπηρετήσει υπηρεσίες πιστοποίησης (Authentication) στα IP data και περιέχει ελέγχους

κρυπτογράφησης. Μπαίνει ανάμεσα στο IP header και τα πακέτα με τα data (payload)χωρίς να τα τροποποιεί .Περιλαμβάνει πέντε πεδία:

- το πεδίο με το Next Header
- το μήκος του payload
- το Security Parameter Index
- τον αριθμό ακολουθίας και
- authentication data

Τα σημαντικά είναι το Security Parameter Index που καθορίζει ποιο είδος από πρωτόκολλα χρησιμοποιούνται και βεβαίως η πιστοποίηση των δεδομένων(authentication data) .

Για να αποτραπεί η υποκλοπή των data κατά τη διάρκεια της επαναμετάδοσης στο AH υπάρχει μηχανισμός antireplay που βοηθά τον μετρητή πακέτων.

γ) Encapsulating Security Payload (ESP).Είναι υπεύθυνο για την κρυπτογράφηση των πακέτων.Το ESH header μπαίνει ανάμεσα στην IP header και των πακέτων με τα data τα οποία όμως και τα τροποποιεί. Περιλαμβάνει τα εξής πεδία :

- το Security Parameter Index ,που δηλώνει στον δέκτη ποιο Security Association(SA) είναι καταλληλότερο για το συγκεκριμένο πακέτο
- το μήκος του payload
- τον αριθμό ακολουθίας ,που προσφέρει προστασία από υποκλοπή κατά τη μετάδοση και αποτρέπει σύγχυση κατά την παραλαβή.
- authentication data.

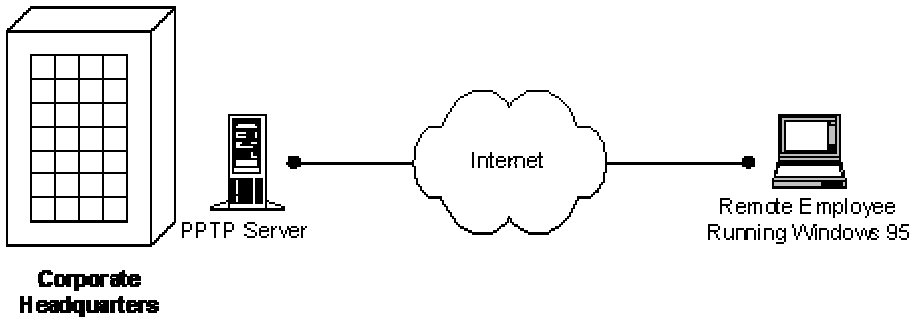
Τρία είναι τα σημεία που πρέπει να εγκατασταθεί IPSec software και σε συνάρτηση με το είδος του VPN που θα δημιουργηθεί : Gateways ,mobile clients και εσωτερικοί χρήστες.

Συνοψίζοντας για το **IPSec** PROTOCOL θα σημειώναμε ότι θεωρείται από τα πιο " πλήρες" αφού περιλαμβάνει έναν αριθμό από αλγορίθμους πιστοποίησης και κρυπτογράφησης καθώς επίσης είναι έτοιμο για μελλοντικές τροποποιήσεις(flexibility, scalability).

3.1.2. PPTP PROTOCOL

Το Point-to-Point Tunneling Protocol (PPTP) δημιουργήθηκε από ομάδα εταιριών που ονομάστηκε PPTP Forum.Συμμετείχαν η η Microsoft ,η 3Com,η US Robotics και η Ascend Communications.

Η βασική ιδέα ήταν να δημιουργηθούν οι προϋποθέσεις για την εύκολη και με ασφάλεια πρόσβαση απομακρυσμένων χρηστών (remote clients) με τα εταιρικά τους δίκτυα, μέσω τοπικού ISP. Βασίστηκε στο PPP που χρησιμοποιείται ευρέως στο Internet.Τα PPP πακέτα ενσωματώνονται (encapsulating) με τη βοήθεια ενός άλλου πρωτοκόλλου του Generic Routing Encapsulation(GRE).Η βασική διαφορά του με το IPSec είναι ότι είναι σχεδιασμένο για το Layer 2 αντί του Layer 3.Έτσι μπορεί να μεταφέρει και άλλα εκτός των IP πακέτων διαμέσω των tunnels.



Εικόνα 4.Το PPTP πρόταση της Microsoft.

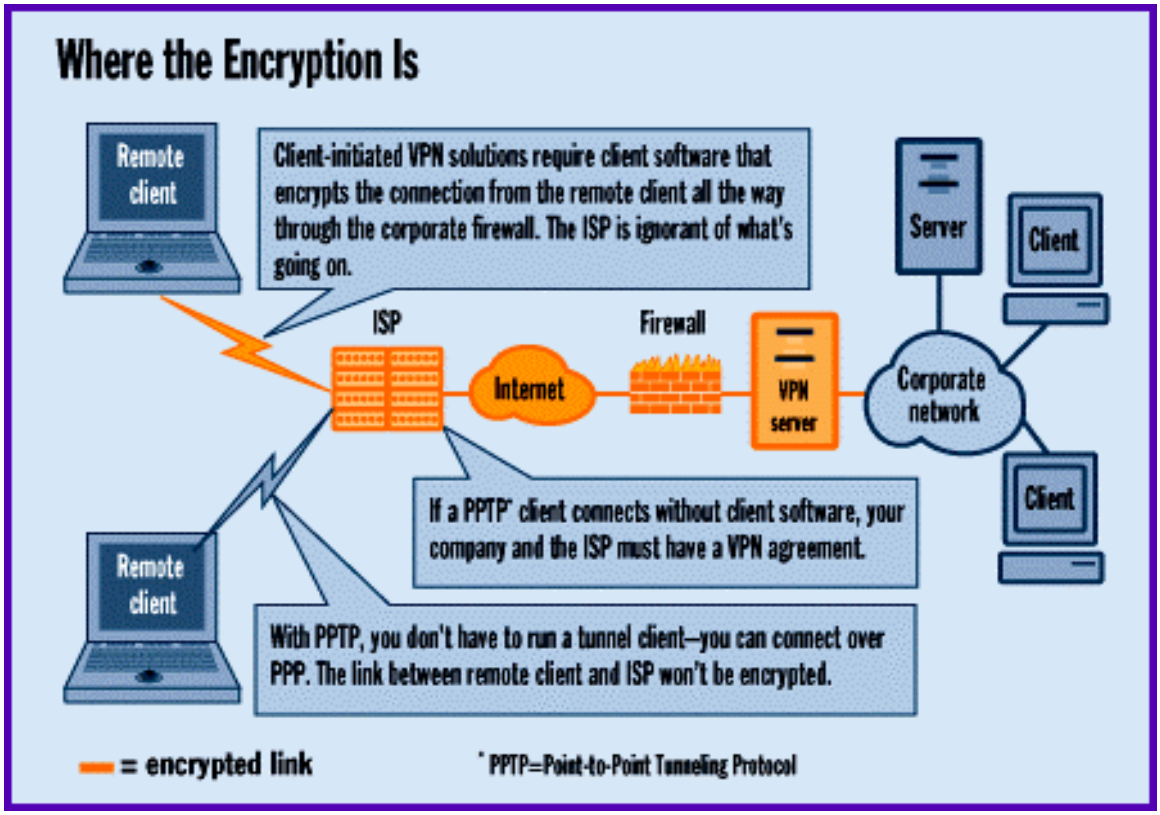
Το PPTP περιμένει από το PPP να κάνει τις εξής ενέργειες:

- Σύνδεση και τερματισμό της φυσικής σύνδεσης.
- Πιστοποίηση ταυτότητας χρήστη
- Δημιουργία PPP datagrams

Αμέσως μετά το PPTP κάνει την ενθυλάκωση (encapsulating).Ορίζει δύο διαφορετικούς τύπους πακέτων τα control packets και τα data packets και τα στέλνει με διαφορετικά κανάλια τα πρώτα μέσω TCP και τα δεύτερα μέσω IP . Τα data πακέτα περιέχουν τα δεδομένα ενώ τα control πακέτα περιέχουν στοιχεία για τη σύνδεση ή πληροφορίες για management και configuration μεταξύ των δύο συνδεδεμένων άκρων. Υπάρχει η δυνατότητα για τη

δημιουργία διαφορετικών τύπων tunnels ανάλογα με τη δυνατότητα του client και του ISP.

Το πρωτόκολλο αυτό είναι από τα δημοφιλέστερα .Ο λόγος είναι ότι είναι στενά δεμένο με τα Win NT , software που τρέχει στους περισσότερους servers.Επίσης έχει ευκολία στη διαχείριση και υποστήριξη πολλών διαφορετικών πλατφορμών λειτουργικών στους remote users. Άλλο σημαντικό του στοιχείο είναι ότι χρησιμοποιώντας RADIUS servers από την πλευρά του ISP προσφέρει αρκετά καλή ασφάλεια που πάντα είναι ζητούμενο .



Εικόνα 5.Το PPTP με VPN software του ISP ή software με του χρήστη.

3.1.3. L2F PROTOCOL

Το 1996 η Cisco έκανε τη δική της πρόταση το πρωτόκολλο Layer Two Forwarding(L2F).Για τη χρήση του χρειάζεται την ύπαρξη Access Server και Router . Επίσης μιας και είναι Client transparent πρέπει ο εξοπλισμός του ISP να το υποστηρίζει. Επιτρέπει πάνω από μία ταυτόχρονες συνδέσεις κατά τη δημιουργία του tunnel.Χρησιμοποιεί το PPP για την πιστοποίηση ταυτότητας του χρήστη αλλά επίσης υποστηρίζει TACACS+ (Terminal Access Controller Access Control System)και RADIUS(Remote Authentication Dial-in User Service). Έχει δύο επίπεδα πιστοποίησης :το πρώτο από το ISP όταν δημιουργεί το tunnel και το δεύτερο όταν γίνεται η σύνδεση με την επιχείρηση.

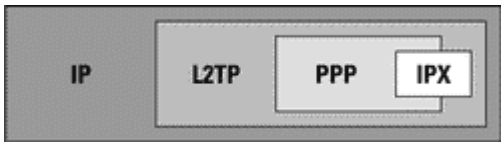
Τα δύο πρωτόκολλα PPTP και L2F και ύστερα από συμφωνία των εταιριών που τα ανέπτυξαν "ενώθηκαν" δημιουργώντας το Layer Two Tunneling Protocol (L2TP).

3.1.4. L2TP PROTOCOL

Θεωρείται το "νέο όπλο" στα VPNs.Συνδυάζει πολλά χαρακτηριστικά και πλεονεκτήματα άλλων πρωτοκόλλων και επίσης την υποστήριξη μεγάλων εταιριών. Βασίζεται στο PPTP και L2F. Είναι ευέλικτο μιας και λειτουργεί στο Δεύτερο επίπεδο του μοντέλου OSI , δίνει τη δυνατότητα χρήσης των IPX ή NETBEUI καθώς επίσης και ATM και Frame relay.

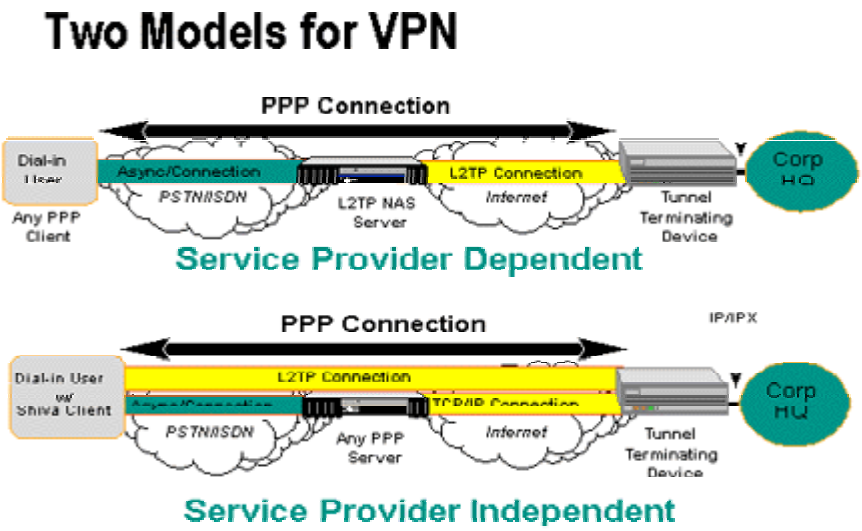
Επειδή χρησιμοποιεί PPP για τις dial –up συνδέσεις συμπεριλαμβάνει τους μηχανισμούς του για την πιστοποίηση καθώς επίσης και άλλους επιπρόσθετους όπως το RADIUS και το IPSec.Η διαδικασία έχει ως εξής:το PPP είναι αυτό που αναλαμβάνει να γίνει η σύνδεση , εκτελεί την πρώτη φάση πιστοποίησης του χρήστη και δημιουργεί τα datagrams. Εδώ αναλαμβάνει το L2TP.Αρχικά επιβεβαιώνει ότι ο εταιρικός server πιστοποιεί την ταυτότητα του remote user και ότι του επιτρέπει τη δημιουργία του tunnel.Όταν το tunnel δημιουργηθεί κάνει ενθυλάκωση (encapsulation)των PPP πακέτων που

μεταδίδονται μέσω του ISP. Επειδή υπάρχει η δυνατότητα για παράλληλη ύπαρξη πολλών συνδέσεων στο ίδιο tunnel , κάθε πακέτο εφοδιάζεται με ένα Call ID που τοποθετείται στην επικεφαλίδα του και χρησιμεύει σαν αναγνωριστικό. Αν πάλι δημιουργηθούν πολλά παράλληλα tunnels τότε επίσης μπαίνει κάποιο αναγνωριστικό που βοηθά τον server της επιχείρησης και αποτρέπει τα λάθη παραλαβής πακέτων .



Όμοια με το PPTP ορίζει δύο διαφορετικούς τύπους πακέτων τα control packets και τα data packets τα στέλνει όμως με ίδιο κανάλι .Τα data πακέτα περιέχουν τα δεδομένα είναι δηλαδή τα αυθεντικά PPP πακέτα του αλλά έχουν και πληροφορίες για το μέσο μετάδοσης (Ethernet, frame re-lay,X.25,ATM) ενώ τα control πακέτα περιέχουν στοιχεία για τη σύνδεση ή πληροφορίες για management και configuration μεταξύ των δύο συνδεδεμένων άκρων.

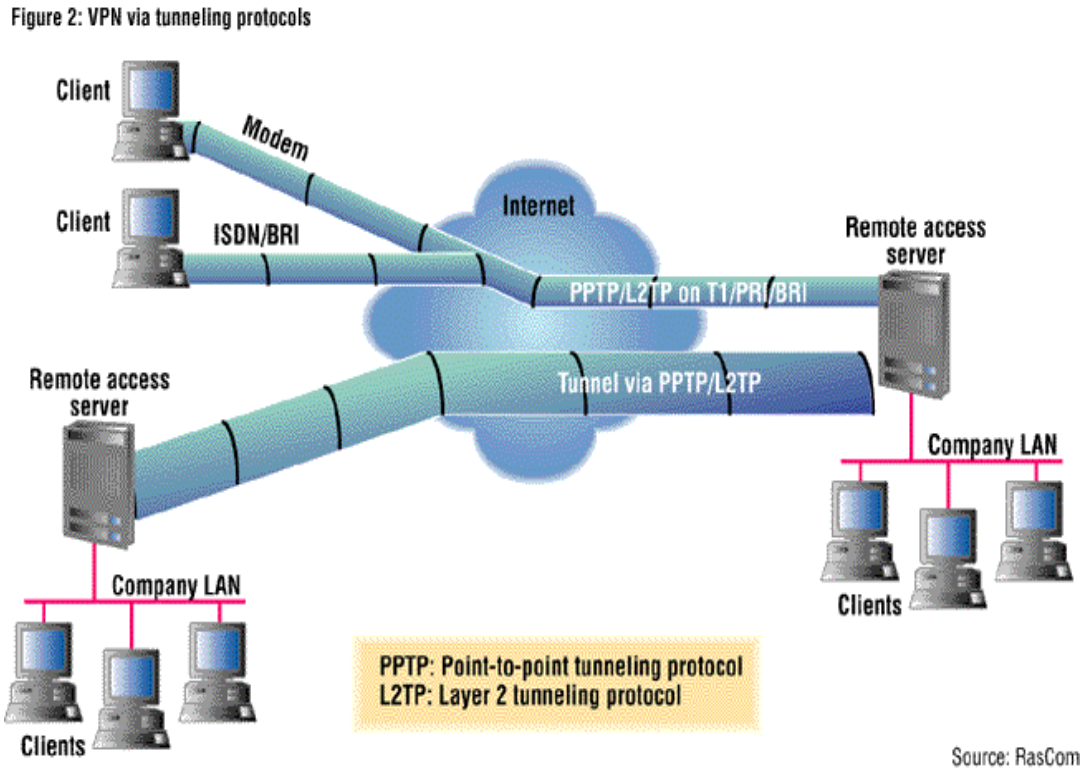
Το L2TP δίνει τη δυνατότητα δημιουργίας δύο τρόπων tunneling.Τα "voluntary" tunnels δημιουργούνται από τον τελικό χρήστη. Ο χρήστης μπορεί ταυτόχρονα να ανοίξει και άλλη σύνδεση χωρίς tunneling με TCP/IP για το Internet.Τα mandatory tunnels είναι user transparent δημιουργούνται δηλ. εν' αγνοία του χρήστη κατά τη διάρκεια της σύνδεσης με τον ISP. Οι συνδέσεις αυτές όμως έχουν προκαθορισμένα άκρα και ως εκ τούτου ο client δεν μπορεί να περιηγηθεί στο Internet.Έχουν το πλεονέκτημα της εύκολης διαχείρισης και της μη φόρτωσης του εσωτερικού δικτύου αλλά και το μειονέκτημα της ασφάλειας αφού το Secure tunnel αρχίζει από τον ISP και μετά.



Εικόνα 6. Δύο τρόποι Tunneling.

Συμπερασματικά θα σημειώναμε πως το L2TP ή το πρωτόκολλο του μέλλοντος για τα VPNs όπως το ονομάζουν συγκεντρώνει τα καλύτερα χαρακτηριστικά των PPTP και L2F.Σημαντικό του πλεονέκτημα είναι πως "τρέχει "

πάνω σε πολλά δίκτυα όπως Frame relay, X25 ή ATM έτσι προσφέρει ευελιξία στον σχεδιασμό(flexibility)και επίσης ασφάλεια επειδή χρησιμοποιεί IPSec και ESP για encryption.



Εικόνα 7. Tunneling πρωτόκολλα

ΣΥΓΚΡΙΣΗ ΠΡΩΤΟΚΟΛΛΩΝ

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

Πίνακας 2. Σύγκριση πρωτοκόλλων

3.2.ΣΧΕΔΙΑΣΜΟΣ

Ο τρόπος ανάπτυξης ενός δικτύου εξαρτάται από πλήθος παραγόντων. Ομαδοποιώντας τους θα διακρίναμε τρείς κατηγορίες : α)οι απαιτήσεις και οι προσδοκίες μας από το δίκτυο, β) οι τρόποι προστασίας των δεδομένων και γ) η γεωγραφική κάλυψη που επιδιώκουμε.

Αρχικά θα πρέπει να ξεκαθαριστούν ερωτήματα όπως :Πόσοι χρήστες θα υπάρχουν; θα είναι και από άλλες χώρες ;τι είδους σύνδεση θα έχουμε με τον ISP;πόσος φόρτος θα υπάρχει στο δίκτυό μας ; θα χρειαστούμε καινούργιο εξοπλισμό και σε τι βαθμό; θα χρειαστεί εξοπλισμός είτε software είτε hardware σε όλους όσους θα συνδέονται στο VPN και τι είδους ; κ. λ. π.

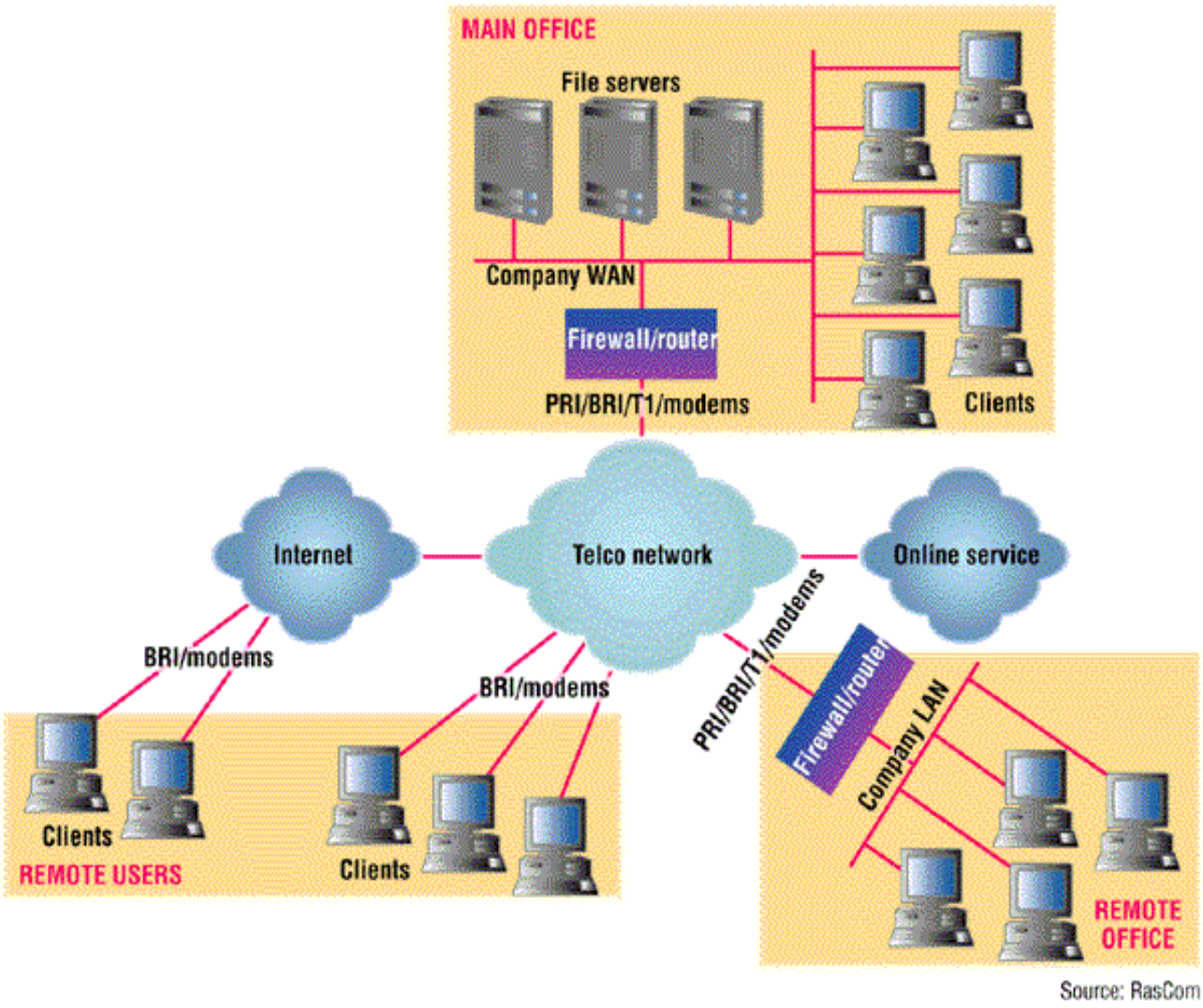
Ειδικά το θέμα του bandwidth του δικτύου είναι από τα σημαντικότερα. Θα διακινούνται εικόνα και ήχος ή απλώς θα ανταλλάσσονται text αρχεία ;Θα υπάρχει τηλεδιάσκεψη; Θα υπάρχει καθυστέρηση στους home users ; Μήπως θα πρέπει να αναβαθμιστεί και το εσωτερικό δίκτυο ;Τι είδους σύνδεση θα απαιτηθεί με τον provider και τι εύρους; Υποστηρίζει VPN;Έχει εξοπλισμό που να παρέχει ασφάλεια ;Και οι users του εξωτερικού πώς θα συνδέονται;

Επίσης πολύ σημαντικό είναι το θέμα της ασφάλειας και προστασίας των δεδομένων αφού θα "ταξιδεύουν" μέσα από ένα επικίνδυνο περιβάλλον. Θα πρέπει να αγοραστεί VPN εξοπλισμός που να παρέχει πρόσθετη προστασία; Θα μπορούσε να υλοποιηθεί μια DMZ(Demilitarized zone)λύση; Δηλαδή η χρησιμοποίηση δύο firewalls ,ο ένας μεταξύ Internet και επιχείρησης και ο άλλος μεταξύ κοινοποιήσιμων και μη στοιχείων μέσα στην επιχείρηση ; Πώς θα συνεργάζονται οι τρόποι πιστοποίησης και κρυπτογράφησης μεταξύ δύο επιχειρήσεων που αποφασίζουν να μετέχουν στο VPN αλλά και να διατηρήσουν τους δικούς τους που ήδη χρησιμοποιούν;

Όλα τα παραπάνω είναι άρρηκτα συνδεδεμένα με το είδος του VPN που πρόκειται να χτιστεί. Κάθε επιλογή επηρεάζει την επιλογή πρωτοκόλλου και κατά συνέπεια την όλη δομή του δικτύου .Και η επιλογή φαίνεται πως

είναι πρωτίστως της διοίκησης της επιχείρησης και δευτερευόντως του τμήματος μηχανογράφησης αφού τις αποφάσεις της πρώτης θα υλοποιήσει η δεύτερη.

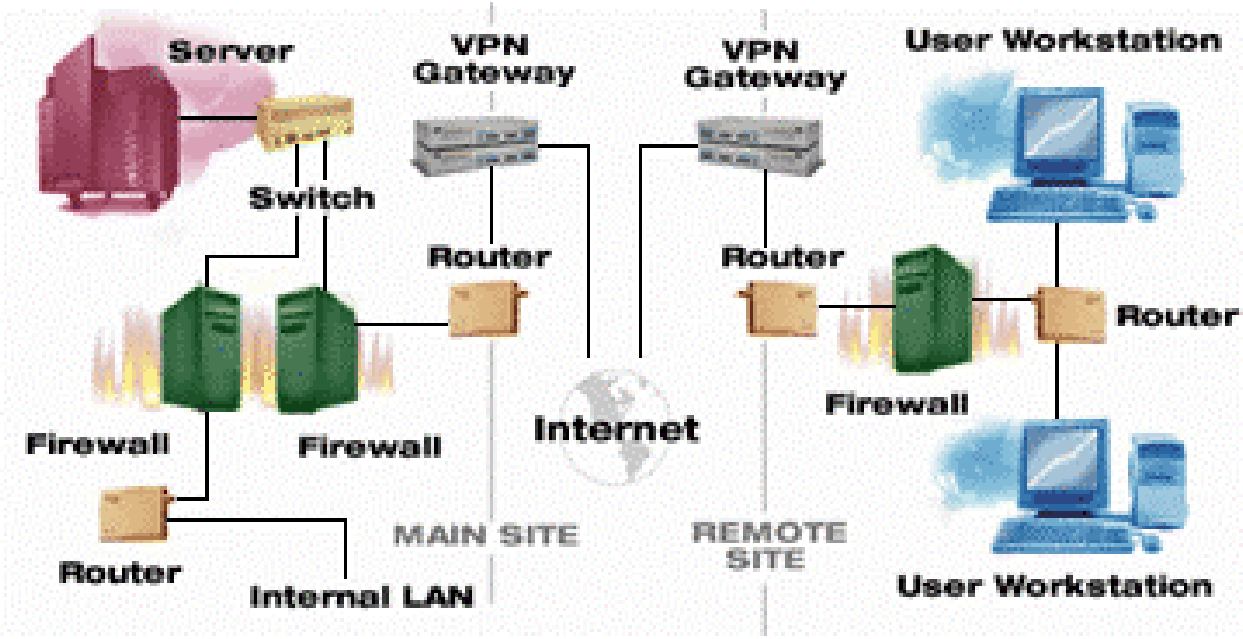
Figure 1: Different VPN deployment strategies



Εικόνα 8. Ανάπτυξη και σχεδιασμός VPN

3.3.ΕΞΟΠΛΙΣΜΟΣ

Όπως ο ορισμός για τα Virtual Private Networks (VPNs) είναι διαφορετικός από εταιρεία σε εταιρεία το ίδιο συμβαίνει και για τον εξοπλισμό που χρησιμοποιείται στην υλοποίησή τους. Υπάρχουν ειδικές συσκευές που παρέχουν υπηρεσίες VPN αλλά και routers ή firewalls που τις υποστηρίζουν .Το VPN software και hardware μπορεί να τοποθετηθεί σε διάφορα σημεία του δικτύου, ανάμεσα στον ISP και το εταιρικό δίκτυο ,πριν τους routers ή ακόμα-ακόμα και αντί αυτών αφού πλέον τους υπερκαλύπτουν.



Εικόνα 9. VPN Εξοπλισμός .

3.3.1.FIREWALLS

Παρόλο που οι firewalls είναι αναπόσπαστο μέρος του δικτύου σε θέματα ασφάλειας δεν είναι ικανοί από μόνοι τους να παρέχουν την ολοκληρωτική ασφάλεια που απαιτείται στα VPNs .Ο λόγος είναι γιατί δεν μπορούν να ελέγξουν την τυχόν αλλαγή που έγινε στα πακέτα δεδομένων κατά τη διάρκεια της μεταφοράς τους στο PSTN (Public Switched Telephone Network).Συνήθως λειτουργούν συμπληρωματικά των άλλων εφαρμογών ασφάλειας αφού επιβλέπουν συνολικά το δίκτυο και προστατεύουν με γενικούς κανόνες και πολιτικές της επιχείρησης. Επισύρουν μεγάλη προσοχή στο στήσιμό τους αφού θεωρούνται περίπλοκοι στο χειρισμό. Μάλιστα και για λόγους καλύτερης διαχείρισης προτείνεται να υπάρχει το ίδιο configuration σε όλους τους firewalls που μετέχουν στο δίκτυο.

Ο συνδυασμός firewall και τύπου VPN είναι σημαντικός. Αν το VPN χρησιμοποιεί τα πρωτόκολλα PPTP και L2TP τότε πρέπει ο firewall να αφήνει να περνούν αυτά τα πακέτα μιας και τα PPTP και L2TP τερματίζονται στον network server.Αν πάλι χρησιμοποιείται το IPSec τότε θα πρέπει να προσεχτεί ο συνδυασμός των δύο αφού υπάρχει περίπτωση ασυμβατότητας των αλγορίθμων και κατά συνέπεια των πρωτοκόλλων. Και στις δύο περιπτώσεις οι remote users θα πρέπει να εφοδιαστούν με ειδικό software συμβατό με αυτό του firewall.

Η λύση με VPNs firewalls αντενδείκνυται σε μεγάλα δίκτυα με υψηλές απαιτήσεις λειτουργεί όμως ικανοποιητικά σε μικρότερα. Γενικά θα λέγαμε πως χρήση firewalls στα VPNs είναι κυρίως συμπληρωματική και όχι αποκλειστική λύση .

3.3.2.ROUTERS

Οι routers (δρομολογητές) είναι επίσης συσκευές που μπορούν να εκπληρώσουν VPNs λειτουργίες. Έτσι κι αλλιώς είναι επιφορτισμένοι να ελέγχουν την κίνηση των πακέτων προς και από το δίκτυο .Για να είναι ικανοί για VPN χρήση θα πρέπει να:

- ενσωματώνουν δυνατότητα για ξεχωριστές συνδέσεις κρυπτογραφημένες και απλές .
- Υποστηρίζουν τους βασικούς IPSec PPTP και L2TP αλγόριθμους.
- Υποστηρίζουν τους transport και tunnel IPSec mode.
- Υποστηρίζουν antireplay μηχανισμούς IPSec2.
- Υποστηρίζουν κρυπτογραφικούς μηχανισμούς.
- Επιτρέπουν επεμβάσεις στο Configuration.

Η αδυναμία τους έγκειται στο ότι δεν είναι σχεδιασμένοι για να παρέχουν και πιστοποίηση ταυτότητας του χρήστη(authentication) οπότε χρειάζονται συμπληρωματικά και authentication server . Επιπροσθέτως οι VPN routers που κυκλοφορούν στην αγορά παρουσιάζουν ιδιομορφίες .Για παράδειγμα το μοντέλο της Intel "Intel Express" χρησιμοποιεί δικό του αλγόριθμο για encryption που σημαίνει ότι για να λειτουργήσει το VPN σε κάθε gateway πρέπει να υπάρχει το μόνο συγκεκριμένο. Τελευταίως όμως οι κατασκευαστές ενσωματώνουν δυνατότητες routing στις VPN συσκευές τους και έτσι μία συσκευή εκτελεί πολλαπλές λειτουργίες .

3.3.3.VPN HARDWARE

Ενώ λοιπόν υπάρχουν προϊόντα που συνδυάζοντας software και hardware παρέχουν υπηρεσίες VPN ,ωστόσο δεν αποτελούν ολοκληρωμένη πρόταση .Έτσι για να στηθεί ένα τέτοιο δίκτυο πρέπει να ενωθούν συσκευές διαφορετικών προσανατολισμών, διαφορετικών κατασκευαστών και ίσως και δυνατοτήτων. Τα προβλήματα που παρουσιάζονται ,έρχονται να καλύψουν εξειδικευμένες συσκευές που εμπεριέχουν όλα όσα χρειάζεται ένα VPN για να λειτουργήσει σωστά χωρίς την προσθήκη software ή hardware στο υπάρχον

υλικό. Πολλές από αυτές όμως περιλαμβάνουν και άλλες δυνατότητες όπως routing ,firewall,DNS και e-mail υπηρεσίες .

Οι συσκευές αυτές χωρίζονται σε δύο μεγάλες κατηγορίες ανάλογα με τον τρόπο δημιουργίας του tunnel και τον τρόπο πρόσβασης: είναι οι LAN-to-LAN και οι dial-in ή αλλιώς remote VPN gateways. Άλλοι κατασκευαστές πάλι κάνοντας διαφορετικό διαχωρισμό ανάλογα με τον τρόπο χρήσης της VPN συσκευής δηλ. αν θεωρούν ότι η συσκευή έχει αποστολή τη φυσική σύνδεση του δικτύου τότε προσφέρουν επιπροσθέτως και διαχείριση πόρων και band-width ενώ αν πιστεύουν ότι η συσκευή έχει σκοπό μόνο τη διαχείριση του δικτύου την εφοδιάζουν με mail servers και DNS caching .

Το να συγκεντρώνονται πολλές υπηρεσίες σε μία συσκευή έχει τα πλεονεκτήματά του όπως εύκολη διαχείριση ή εύκολος έλεγχος αλλά βεβαίως υπάρχει ο φόβος αν κάτι δεν πάει καλά να χαθούν όλες οι λειτουργίες (single point of failure).

Χτίζοντας ένα VPN δίκτυο θα πρέπει να δώσουμε περισσότερη έμφαση σε τέσσερα σημεία:Tunneling,κρυπτογράφηση ,πιστοποίηση χρηστών και διαχείριση. Πάλι όμως και σε συνάρτηση με το ποια από αυτές τις λειτουργίες θεωρούμε σημαντικότερη θα επιλέξουμε συσκευή που θα υποστηρίζει το ανάλογο πρωτόκολλο δηλ. PPTP , L2TP ή IPSec.Το PPTP για παράδειγμα δίνει έμφαση στο tunneling και παρέχει μικρή κρυπτογράφηση, ενώ το L2TP υποστηρίζει δυνατή πιστοποίηση ταυτότητας και το IPSec δίνει μεγάλη ασφάλεια.

Θα πρέπει επίσης να προσεχτεί το γεγονός ότι οι remote users δημιουργούν για κάθε σύνδεση ένα tunnel.Πρέπει λοιπόν να υπολογιστεί ο αριθμός των ταυτόχρονων συνδέσεων δηλ. ταυτόχρονων ανοιχτών καναλιών γιατί παίζει ρόλο στην επιλογή της συσκευής (κάθε μοντέλο υποστηρίζει διαφορετικό αριθμό).

Συμπερασματικά θα τονίζαμε ότι η επιλογή της καταλληλότερης συσκευής είναι πρωτίστως συνάρτηση του μεγέθους της επιχείρησης που θέλουμε να καλύψουμε .Για μικρές επιχειρήσεις με λίγα γραφεία και λίγο προσωπικό οι συσκευές που προσφέρουν πολλές υπηρεσίες είναι κατάλληλες .Ίσως η απόδοσή τους να μην είναι η ανώτερη δυνατή αλλά τα

πλεονεκτήματά τους τις κάνουν ελκυστικότερη λύση. Από την άλλη αν η επιχείρηση είναι μεγαλύτερη τότε δημιουργούνται διλήμματα. Ο προσανατολισμός της επιχείρησης είναι το κριτήριο για την επιλογή μιας all in one συσκευής με εξειδίκευση στην ασφάλεια ή το tunneling κ.λ.π ή μιας άλλης λύσης πιο σύνθετης .

3.3.4.VPN SOFTWARE

Τα προϊόντα που ανήκουν σ΄αυτήν την κατηγορία κατηγοριοποιούνται ως εξής: α) προϊόντα που χρησιμοποιούνται για LAN-to-LAN VPN συνδέσεις και β)για χρήση host to host tunneling .Η αγορά προσφέρει κυρίως τα πρώτα με δυνατότητες για χρήση πολλών VPN ταυτόχρονα ή ακόμα και διαχείρισης των δικτύων αυτών παρ' όλα αυτά όμως υπάρχουν και ειδικά software για Host – to- host συνδέσεις με εξαιρετικά αποτελέσματα.

Όμως εδώ υπάρχουν και προιόντα τα οποία χρησιμοποιούν και άλλες μεθόδους ενθυλάκωσης (encapsulation) των πακέτων και Tunneling εκτός των ήδη αναφερθέντων.Τέτοια είναι το SOCKS v5 ή το Secure Shell (SSH) τα οποία χρησιμοποιούνται σε άλλες εφαρμογές για παράδειγμα από την NASA ή μεγάλες τράπεζες.

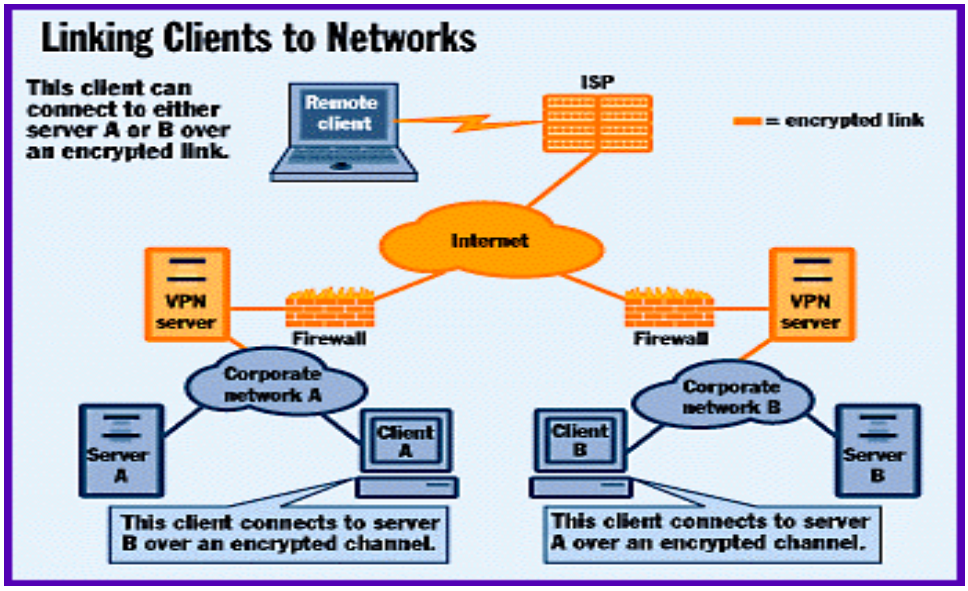
Δύο μεγάλες εταιρείες κατασκευής λειτουργικών συστημάτων όμως η Microsoft και η Novell συμπεριλαμβάνουν VPN software στα λειτουργικά τους. Η Microsoft το PPTP στο Routing and Remote Access Server(RRAS) των WinNT και η Novell το RC2 στο προϊόν Borderguard του NetWare.Υπάρχει και εδώ το δίλημμα για την ορθότητα της απόφασης πολλών υπηρεσιών σε ένα μηχάνημα εν προκειμένω στον server με τα αντίστοιχα θετικά και αρνητικά του σημεία . Επιπροσθέτως τίθεται και το θέμα της απόδοσης του hardware με την ταυτόχρονη ανάθεση πολλών εργασιών σε ένα μοναδικό μηχάνημα.

Όσον αφορά το host-to-host VPN software δεν υπάρχουν πολλά προϊόντα διότι κατ' αρχήν η όλη διαδικασία συμπεριλαμβανόμενης και της κρυπτογράφησης και αποκρυπτογράφησης καθυστερεί τους stand alone υπολογιστές, αλλά και γιατί η διαχείριση και η ασφάλεια είναι ευκολότερη όταν γίνεται από ένα σημείο όπως Router ή Firewall. Παρ' όλα αυτά για αυτού του

είδους το software χρησιμοποιείται ευρέως το IPSec μιας και δίνει τη μεγαλύτερη ασφάλεια .

Γενικά τα σημεία που θα πρέπει να προσεχτούν στο VPN software είναι:

- Τα πρωτόκολλα που υποστηρίζονται.
- Η χωρίς προβλήματα συνύπαρξη με υπάρχον λογισμικό (no conflicts).
- Θέματα ασφάλειας όπως κρυπτογράφηση και πιστοποίηση ταυτότητας χρηστών.
- Διαχείριση (δυνατότητα για remote management) .
- Auditing.



Εικόνα 9. Πλάνο ανάπτυξης

4. Η ΔΙΑΧΕΙΡΙΣΗ ΕΝΟΣ VPN

Ανεξάρτητα με το πόσα χαρακτηριστικά έχει μια υπηρεσία ,πόσο καλά αποδίδει και πόσο εξυπηρετεί τις ανάγκες ενός οργανισμού, δεν είναι ποτέ ιδανική εκτός αν είναι εύκολη στη διαχείριση και με χαρακτηριστικά που βοηθούν τον διαχειριστή να εξάγει τα στοιχεία που χρειάζονται. Από τα βασικά

στοιχεία διαχείρισης ενός VPN δικτύου είναι η ασφάλεια, η διευθυνσιοδότηση (IP Addressing),και η γενικότερη απόδοση του δικτύου.

4.1. ΑΣΦΑΛΕΙΑ

Επιγραμματικά θα μπορούσαμε να πούμε για τα ζητήματα ασφαλείας που άπτονται του θέματος ότι:

α)τα θέματα αυτά εμπίπτουν στη γενική πολιτική της εταιρίας δηλαδή για το ποια στοιχεία της είναι σημαντικά, ποια θέλει να προστατεύσει ,από ποιους , με ποιο κόστος κ.λ.π.

β) η απόφαση για τον τρόπο ασφάλειας είναι συνάρτηση της επιλογής VPN συσκευών ή software και βεβαίως πρωτοκόλλων που υποστηρίζονται από αυτά. Το PPTP για παράδειγμα παρέχει μικρή κρυπτογράφηση, ενώ το L2TP υποστηρίζει δυνατή πιστοποίηση ταυτότητας και το IPSec δίνει τη μεγαλύτερη ασφάλεια σχετικά με τα άλλα. Σχετικό με τα παραπάνω και τους αλγόριθμους που χρησιμοποιούνται , είναι το "μήκος κλειδιού σε bits"(key length in bits)που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Ο παρακάτω πίνακας δίνει μια ιδέα συγκρίνοντας το μήκος κλειδιού και το χρόνο που απαιτείται για να σπάσει με τα μέχρι τώρα γνωστά μέσα και μεθόδους .

40 bits	56 bits	64 bits	80 bits	128 bits
2 seconds	35 hours	1 year	70.000 years	10^{19}years

Είναι λοιπόν προφανές ότι η ασφάλεια του VPN εμπίπτει στη γενικότερη πολιτική της επιχείρησης για το τι είναι σημαντικό και τι όχι, για το ποιος έχει πρόσβαση και πού και βεβαίως για το πόσα χρήματα κρίνεται απαραίτητο να δαπανηθούν για το σκοπό αυτό.

4.2. IP ADDRESS MANAGEMENT

Η χρήση του πρωτοκόλλου IP στις επικοινωνίες σηματοδότησε μια νέα εποχή για την ανάπτυξή τους .Παρ΄όλα αυτά όμως δεν είναι χωρίς προβλήματα κυρίως σε θέματα κατανομής και διαχείρισης .Βεβαίως το ζήτημα

θα είναι μεγαλύτερο τα επόμενα χρόνια όπου όπως φαίνεται "τελειώνουν" οι διευθύνσεις στο Internet οπότε και για να καλυφθούν οι ανάγκες δημιουργήται το IPv6 με 128 bits αντί του υπάρχοντος IPv4 με 32 bits.

Πως όμως γίνεται η η διευθυνσιοδότηση (IP Addressing)μέχρι τώρα ; Σε μια μεγάλη επιχείριση με πολλούς υπολογιστές, servers και άλλες συσκευές που απαιτούν IP διεύθυνση, το να προσθέσεις ,να μετακινήσεις ή να αλλάξεις μια συσκευή είναι μεγάλο πρόβλημα. Είναι δύσκολο επίσης να ελέγξεις για λάθη συστήματος προερχόμενα από το IP. Πολλές φορές δίνεται τι ίδιο IP address σε δύο ή περισσότερους χρήστες με συνέπεια προβλήματα στο routing αλλά και στις εφαρμογές .Όταν πάλι υπάρχουν στελέχη που συνεχώς ταξιδεύουν και αναγκαστικά έχουν πολλαπλά IP addresses για πρόσβαση σε διαφορετικούς Access servers αυτό δεν είναι το ευχρηστότερο δυνατό. Για να ξεπεραστούν λοιπόν τα προβλήματα της στατικής διευθυνσιοδότησης επινοήθηκε η μέθοδος που ονομάζεται DHCP (Dynamic Host Control Protocol).Οι servers πλέον αναλαμβάνουν αυτόματα να δίνουν δυναμικά ,διευθύνσεις στους χρήστες. Σε εξέλιξη του DNS (Domain Name Service) το οποίο λειτουργούσε μόνο με στατικές IP διευθύνσεις αναπτύχθηκε το DDNS(Dynamic DNS) .Έτσι με το DHCP και το DDNS απλοποιείται η διαχείριση του δικτύου.

Εδώ όμως και καθώς αναπτύσσονται νέες μέθοδοι πιο περίπλοκοι, αναδύονται νέα προβλήματα που σχετίζονται με τα VPNs. Πολλές συσκευές ασφάλειας δικτύων (firewalls, routers) λειτουργούν με στατικές διευθύνσεις. Άλλες πάλι αναγνωρίζουν μόνο διεύθυνση χωρίς να την συνδυάζουν με χρήστη υποθέτοντας ότι η IP address χαρακτηρίζει ένα και μόνο υπολογιστή. Έτσι όμως μπορεί να επιτευχθεί πρόσβαση στο δίκτυο από εξουσιοδοτημένη θέση (IP address) αλλά μη εξουσιοδοτημένο χρήστη. Υπάρχει βεβαίως και η μικτή λύση του DHCP χωρίς DDNS που σημαίνει ότι μερικές διευθύνσεις όπως servers , mail servers κ.λ.π. είναι σταθερές ενώ οι άλλες μοιράζονται δυναμικά.

Αφού όμως το VPN έχει σαν σκοπό και την πρόσβαση σε πηγές της επιχείρησης από στελέχη, ή πελάτες ή άλλους μέσω του Internet ,αυτό δεν είναι επικίνδυνο; Πως θα διαφυλαχθεί το απόρρητο των άλλων πηγών; Μπορεί

να γίνει κάτι σε επίπεδο διαχείρισης δικτύου για τον εκμηδενισμό των διαρροών; Υπάρχουν αρκετές λύσεις με δημοφιλέστερη τη δημιουργία δύο διαφορετικών DNS servers ενός εσωτερικού και ενός εξωτερικού του firewall.Έτσι προφυλάσσονται τα στοιχεία από υποκλοπές.

Ένας άλλος τομέας που ερευνάται είναι της συνεργασίας των VPN συσκευών με NAT software.Το NAT είναι μία λύση για να παρακαμφθεί το πρόβλημα που συναντάται κυρίως στα Extranets :υπάρχει το εσωτερικό δίκτυο με δικές του διευθύνσεις αλλά υπάρχει και σύνδεση με το Διαδίκτυο. Άλλες διευθύνσεις για τους εσωτερικούς και άλλες για τους εξωτερικούς χρήστες είναι δύσκολο να συνυπάρξουν. Το NAT μετατρέπει τις εσωτερικές διευθύνσεις σε τέτοιες που να έχουν νόημα για τον "έξω" κόσμο το Internet δηλαδή. Ο τρόπος όμως που επηρεάζει τα VPNs και βεβαίως λόγω της πολυπλοκότητας που παρουσιάζει είναι θέμα προς διερεύνηση από ομάδες της IEFT .

4.3. PERFORMANCE MANAGER

Είναι προφανές ότι καλή απόδοση έχει ένα δίκτυο κυρίως όταν γρήγορα και χωρίς προβλήματα καλύπτει τις ανάγκες των χρηστών. Τα τελευταία χρόνια όμως ο αριθμός των χρηστών μεγάλωσε και οι ανάγκες τους αυξήθηκαν. Ενώ παλιότερα το FTP ή το e-mail ήταν οι κυριότερες απαιτήσεις τώρα υπάρχουν νέες "βαριές "εφαρμογές, ανταλλαγή multimedia , videoconferencing ή τηλεφωνία μέσω Internet.Τα κυριότερα προβλήματα είναι η καθυστέρηση στην εκπομπή και απάντηση των πακέτων δεδομένων και η καθυστέρηση στην δρομολόγηση των πακέτων αυτών μέσω των συσκευών (routers κ.λ.π.).Οι τρόποι που το VPN χρησιμοποιεί για να αντεπεξέλθει είναι ίδιοι όπως για τα κοινά δίκτυα:

- Bandwidth compression.Αυξάνεται η απόδοση του δικτύου με μεθόδους συμπίεσης που εφαρμόζονται από τους routers.
- Bandwidth on-demand .Όταν αυξάνονται οι ανάγκες του δικτύου χρησιμοποιούνται άλλες πηγές για επιπλέον bandwidth.
- Ip multicasting . Μείωση του επιπρόσθετου φόρτου.

- Class of service. Οι routers με κάποιο ειδικό software αναγνωρίζουν διαβαθμίσεις που έχουν δοθεί σε πακέτα ανάλογα με την πηγή τους και εξυπηρετούν πρώτα αυτά.
- Static resource allocation. Δεσμεύεται μέρος του bandwidth για συγκεκριμένες εφαρμογές ή χρήστες ή πρωτόκολλα κ.λ.π.
- Dynamic resource allocation.Νέα τεχνική πολλά υποσχόμενη που συνδυάζει προηγούμενες.

Ένας άλλος τομέας που ενδέχεται να επηρεάζει τη απόδοση ενός VPN είναι ο ISP αφου χρησιμοποιείται το δικό του τηλεπικοινωνιακό υλικό για τις συνδέσεις μεταξύ των διαφόρων σημείων. Βεβαίως θεωρείται φυσικό πως η ισχύς των συσκευών που χρησιμοποιούνται παίζει σημαντικό ρόλο καθώς επίσης και κάθε λογής Load Balancing ανάμεσά τους.

Τέλος σημασία μπορεί να παίξει και το VPN πρωτόκολλο που χρησιμοποιείται καθότι το L2TP μπορεί να λειτουργεί σε παράλληλα sessions μέσα στο ίδιο tunnel.Έτσι όμως μπορεί να υπάρξει αφενός υπερφόρτωση ,αφετέρου μπέρδεμα με τις πολιτικές αποφόρτισης του δικτύου που προαναφέρθηκαν.

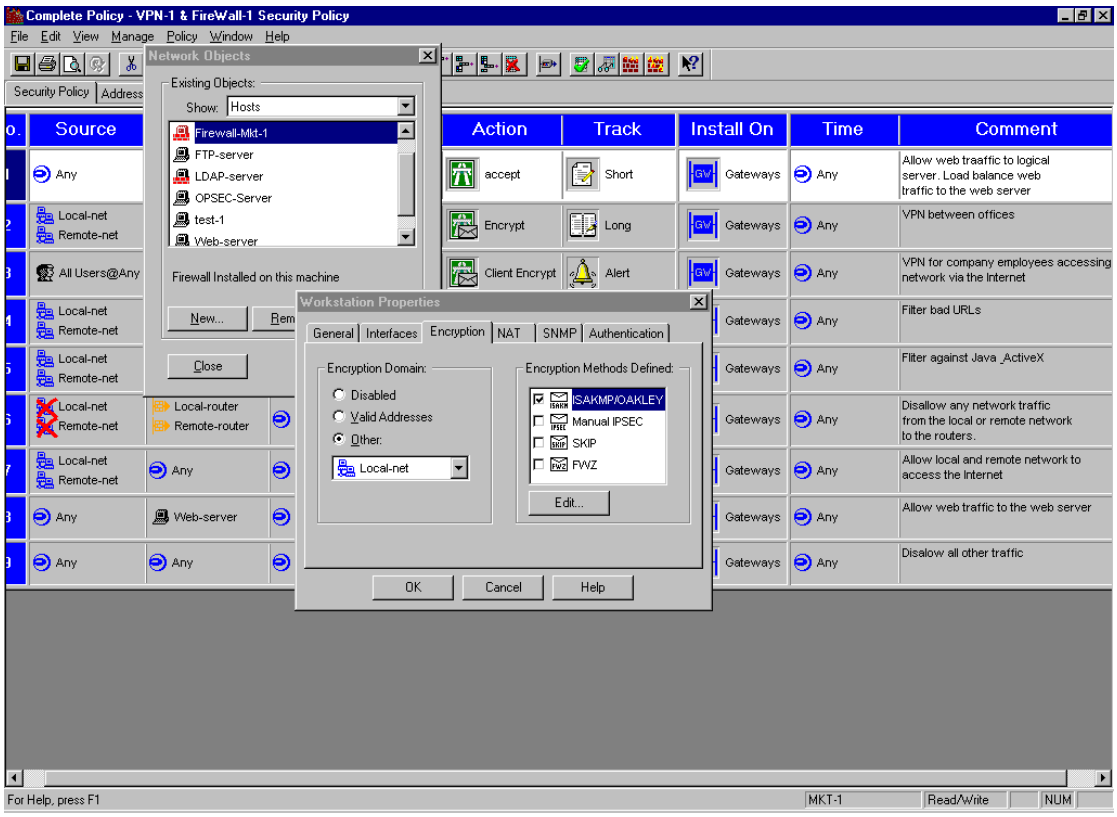
4.4. ΠΟΛΙΤΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΠΙΒΛΕΨΗΣ

Βεβαίως παραπάνω αναλύσαμε πολιτικές που ακολουθεί ο διαχειριστής σε θέματα ασφάλειας ή διαχείρισης του bandwidth ή πρόσβασης στους πόρους του συστήματος . Αυτοί όμως είναι αποσπασματικοί και όχι τόσο αποτελεσματικοί λόγω αυτής τους της ιδιομορφίας .Καθώς λοιπόν τα δίκτυα μεγάλωσαν σε μέγεθος και έγιναν περισσότερο πολύπλοκα, με περισσότερες υπηρεσίες και εφαρμογές ,δημιουργήθηκε η ανάγκη για ολοκληρωτική και από ένα κεντρικό σημείο διαχείριση όλων των ανωτέρω. Η δυνατότητα για γρήγορη διάγνωση και επιδιόρθωση λαθών χωρίς μετακινήσεις και διακοπή της ροής της εργασίας είναι πλέον εκ των ουκ άνεφ για τη σύγχρονη επιχείρηση.

Οι μεγάλες εταιρείες λοιπόν(Cisco ,3Com ,Bay Networks) ανέπτυξαν συστήματα διαχείρισης (policy-based network management) που

διευκολύνουν τον διαχειριστή να μπορέσει να συστηματοποιήσει τη δουλειά του και να προστατέψει πιο αποτελεσματικά το δίκτυό του .Με ειδικό software λοιπόν ορίζει κανόνες που έχουν γενική εφαρμογή και εύκολη διάχυση καθώς "έξυπνες" συσκευές (π.χ. routers) τους εφαρμόζουν προς τους πόρους (top down εφαρμογή). Για παράδειγμα η συνήθης τακτική είναι να δημιουργείται ένας πίνακας δύο ή τριών διαστάσεων με στοιχεία όπως α)το είδος της εφαρμογής β)το χρήστη και γ)κάποιο άλλο σημαντικό στοιχείο όπως η προέλευση ή ακόμα και η ώρα . Ο συνδυασμός αυτών των παραμέτρων δίδει προτεραιότητες εκτέλεσης των εργασιών και εξυπηρέτησης των χρηστών.

Η επόμενη γενιά τέτοιων έξυπνων εργαλείων ήδη δημιουργείται από τη συνεργασία Microsoft και Cisco. Ονομάζεται DEN Initiative(Directory-Enable Networking.Οι συσκευές θα μπορούν μόνες τους να αποφασίζουν για το bandwidth ,την κατανομή των πόρων κ.λ.π σύμφωνα με κανόνες που έχουν οριστεί και κατόπιν αποθηκευτεί στο DEN directory.



Εικόνα 10. Εφαρμογή με Policy-based network management

5. ΕΠΙΛΟΓΟΣ

Τα ¨Εικονικά Ιδιωτικά Δίκτυα¨ (Virtual Private Networks-VPNs) ή αλλιώς Very Profitable Networks όπως προτιμούν πολλοί να τα ονομάζουν ,θα έχουν τεράστια ανάπτυξη τα ερχόμενα χρόνια. Γενικά ό όρος αναφέρεται στα εσωτερικά ή εξωτερικά δίκτυα εταιριών (Intranets και Extranets) τα οποία χρησιμοποιούν το δημόσιο δίκτυο (Public Switched Telephone Network) ως κύριο μέσο επικοινωνίας ,για την μεταφορά των στοιχείων τους .Τα VPNs προσφέρουν πλεονεκτήματα που τα κάνουν σημαντικό και αναπόσπαστο στοιχείο ανάπτυξης των επιχειρήσεων που θέλουν να έχουν στατηγικό πλεονέκτημα στην αγορά. Προσφέρουν:

- Χαμηλό κόστος : στις τηλεπικοινωνίες γιατί οι γραμμές σύνδεσης σε τοπικό παροχέα Internet (ISP) στοιχίζουν πολύ λιγότερο από τις ISDN ή τις ευθείες γραμμές (Leased) και η διασύνδεση μπορεί να γίνει από παντού χωρίς ιδιαίτερο εξοπλισμό. Στη συντήρηση και διαχείριση του δικτύου , μιας και το κόστος το επωμίζεται ο ISP. Στον τηλεπικοινωνιακό εξοπλισμό ,λόγω μικρότερων απαιτήσεων.
- Ευκαμψία μιας και στα παραδοσιακά δίκτυα έπρεπε να υπάρχει συμβατός εξοπλισμός που να υποστηρίζει όλα τα περιφεριακά γραφεία ή τους απομακρυσμένους κλάδους της επιχείρησης ενώ στα VPN’s δεν υπάρχει περιορισμός ή προβλήματα ασυμβατότητας εξοπλισμού αφού απλά και μόνο η σύνδεση με έναν ISP αρκεί για την επικοινωνία.
- Επεκτασιμότητα διότι μέσω του Internet πολύ εύκολα και από οποιοδήποτε μέρος του κόσμου πελάτες , προμηθευτές ή άνθρωποι της επιχείρησης συνδέονται χωρίς δυσκολία με αυτήν .Οι συνδέσεις

αυτές είναι εύκολα αναβαθμίσιμες χωρίς υποχρεωτική αναβάθμιση του εξοπλισμού σε κάθε σημείο (point) αφού αλλάζει μόνο το είδος της σύνδεσης με τον ISP.

- Εύκολη και συγκεντρωτική διαχείριση του δικτύου διότι από ένα σημείο ελέγχονται IP addressing, πολιτικές πρόσβασης χρηστών, ασφάλεια και άλλες συναφείς εργασίες .

- Αυξημένη ασφάλεια λόγω των πρωτοκόλλων tunneling και ασφαλείας που χρησιμοποιούνται στην VPN τεχνολογία.

Συμπερασματικά θα τονίζαμε πως λόγω των μεγάλων πλεονεκτημάτων τους και της ραγδαίας ανάπτυξης του Internet ,τα VPNs αναμένεται να κυριαρχήσουν και να αποτελέσουν standard για το χτίσιμο επιχειρησιακών και εμπορικών δικτύων στο εγγύτατο μέλλον.

6. ΠΗΓΕΣ-ΒΙΒΛΙΟΓΡΑΦΙΑ

1. IEFT Internet Draft-Bhattacharya"IPSec Policy Data Model"
2. IEFT Internet Draft-Doraswamy,Naganand"Implementation of Virtual Private Networks with IP Security"
3. IEFT Internet Draft-Aboba B.Patel"Securing L2TP Using IPSEC"
4. IEFT Internet Draft-Peirce,Ken,Calhoun "Layer Two Tunneling Protocol"
5. IEFT Internet Draft-Bhattacharya"IPSec Policy Data Model"
6. IEFT Internet Draft-Zorn,Glen,Pall "Microsoft Point to Point Encryption"
7. Internet Draft -Valencia,Hamzeh "Layer Two Tunneling Protocol"
8. Dave Kosiur "Building Virtual Private Networks"
9. Network World -Alex Henthorn-"Sorting throught the VPN protocols".
10. PC Week-Lauren G.Paul "Tunnel Vision"

INTERNET

1. **www.ietf.org/** - The Internet Engineering Task Force-Internet Drafts και RCF pages
2. **www.nortelnetworks.com** -Εταιρεία Δικτυακών λύσεων με προϊόντα , υπηρεσίες ,ολοκληρωμένες λύσεις κ.λ.π
3. **www.microsoft.com** -Πληροφορίες για το PPTP-
4. **www.bay.com** -Εταιρεία Δικτυακών λύσεων με προϊόντα , υπηρεσίες, ολοκληρωμένες λύσεις κ.λ.π
5. **www.3com.com**- Εταιρεία Δικτυακών λύσεων με προϊόντα, υπηρεσίες, ολοκληρωμένες λύσεις κ.λ.π
6. **www.checkpoint.com**- Εταιρεία Δικτυακών λύσεων με προϊόντα, ολοκληρωμένες λύσεις κ.λ.π
7. **www.cisco.com**- Εταιρεία Δικτυακών λύσεων με προϊόντα , υπηρεσίες, ολοκληρωμένες λύσεις κ.λ.π
8. **www.intel.com**- Προϊόντα VPN
9. **www.shiva.com**- Εταιρεία Δικτυακών λύσεων με προϊόντα, υπηρεσίες, ολοκληρωμένες λύσεις κ.λ.π
10. **www.vpnet.com**- Εταιρεία VPN λύσεων με προιόντα, ολοκληρωμένες λύσεις κ.λ.π
11. **www.wiley.com**-Εκδοτικός Οργανισμός-Βιβλία για VPN και links σε προϊόντα ,υπηρεσίες, VPN tests, Internet Drafts και RCF pages κ.λ.π.
12. **www.signal9.com**- Εταιρεία Δικτυακών λύσεων με προϊόντα (firewalls,VPNs κ.λ.π)

13. **www.oms.co.za** -Internet solutions,VPNs προϊόντα
14. **www.techweb.com** -Site με πληροφορίες, άρθρα ,links κ.λ.π.για τεχνικά θέματα σε υπολογιστές ,Δίκτυα,Internet κ.α.
15. **www.informationweek.com** -Site με πληροφορίες, άρθρα ,white papers,links κ.λ.π.για τεχνικά θέματα σε υπολογιστές ,Δίκτυα,Internet κ.α.
16. **www.intranetjournal.com** -Site με πληροφορίες, άρθρα ,links κ.λ.π.για τεχνικά θέματα σε υπολογιστές ,Δίκτυα,Internet κ.α.
17. **www.oneboxnetworks.com** - Εταιρεία Δικτυακών λύσεων με προϊόντα, υπηρεσίες, ολοκληρωμένες λύσεις κ.λ.π
18. **www.lcs.mit.edu** - (MIT)Massachusetts Institute of Technology's Laboratory for Computer Science (LCS) Cairin VPN
19. **www.ascend.com** - Lucent Technologies-Εταιρεία Δικτυακών λύσεων με προϊόντα, υπηρεσίες ,ολοκληρωμένες λύσεις κ.λ.π
20. **www.summitonline.com**-Information source about enterprise management available today. Περιλαμβάνει white papers,προιόντα ,press releases σχετικά με enterprise management.
21. **www.tradewave.com** -Η εταιρία TradeWave ασχολείται με το ηλεκτρονικό εμπόριο(EC) σε όλα τα επίπεδά του και προσφέρει Software και hardware λύσεις .
22. **www.psgroup.com** - Η εταιρεία Patricia Seybold είναι consulting firm σε θέματα e-business και τεχνολογίας. Πουλά προϊόντα και παρέχει τεχνογνωσία και συμβουλές σε θέματα τεχνολογίας, ηλεκτρονικού εμπορίου , δικτυακών εφαρμογών κ.λ.π.
23. **www.hilgraeve.com**-Η Hilgraeve είναι εταιρεία παροχής ολοκληρωμένων τηλεπικοινωνιακών υπηρεσιών(Software και hardware) .
24. **www.elmail.co.uk**- Η Kewill E-Commerce Infrastructure είναι εταιρεία παροχής ολοκληρωμένων Internet λύσεων (τηλεπικοινωνιακών υπηρεσιών,Software hardware , ειδική σε ασφάλεια) .
25. **www.masnet.net**- Η MAS NET είναι εταιρεία παροχής ολοκληρωμένων τηλεπικοινωνιακών λύσεων με εξειδίκευση στο Internet.
26. **www.computerworld.com**-Ηλεκτρονική εφημερίδα με πληροφορίες , υπηρεσίες αναζήτησης ,εκδόσεις , papers κλπ .
27. **www.info-sec.com**- Site που ασχολείται με την ασφάλεια. Παρέχει συμβουλές ,πληροφορίες ,πουλά Software και Hardware, βιβλία κ.α
28. **www.americasnetwork.com**-Έχει εκδόσεις στο Internet και με τον κλασσικό τρόπο σε ότι αφορά τα δίκτυα.
29. **www.epm.ornl.gov**- Ερευνητικό κέντρο με θέμα εφαρμοσμένα μαθηματικά και computers science.
30. **www.verio.com** - Παροχέας υπηρεσιών Internet,λύσεις Ηλεκτρονικού εμπορίου , VPNs κλπ.
31. **www.extranet-strategist.com** -Site που ασχολείται με extranets κατά κύριο λόγο. Παρέχει πληροφορίες ,white papers ,πουλά Software και Hardware, βιβλία κ.α