VPN ARCHITECTURES

DAFOULIS SOTIRIOS

2005 , JANUARY

UNIVERSITY OF MACEDONIA
Master Information Systems (MIS)
Networking Technologies
Professors: A. A. Economides & A. Pomportsis

ΟΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΤΩΝ ΕΙΚΟΝΙΚΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ (VPN)

ΝΤΑΦΟΥΛΗΣ ΣΩΤΗΡΙΟΣ

ΙΑΝΟΥΑΡΙΟΣ , 2005

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΜΣ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Καθηγητές : Α. Α. Οικονομίδης & Α. Πομπόρτσης

SUMMARY

According to a commonly accepted definition for VPN, supplied by the IT Governance Institute, VPN is defined as a network of virtual circuits that carries private traffic through public or shared networks such as the Internet or those provided by network service providers (NSPs) . In the VPN terminology the terms "tunnel" or "tunneling" are often used since the definition of these two terms corresponds to the general philosophy on which VPN is based in order to work . As far as "tunneling" is concerned , the process of encapsulating one type of packet in another packet type so the data can be transferred across paths that otherwise would not transmit the data is called tunneling . The paths the encapsulated packets follow in an Internet VPN are called tunnels .

In general , an organization has to decide about which of the VPN models is appropriate to its needs , however there are three common VPN models that applies to the majority of American and European organizations .They are Pure Provider Model , Hybrid Provider Model and End-to-End Model .

In most circumstances VPN plays the role of a single logical network that is used by geographically distributed organizations in order to communicate among them . In addition , VPN must permit mobile employees to access the organization' s intranet , via the Internet , using a secure network communications . In this case VPN is used in combination with dial-up , wireless and broadband ISPs . Apart from providing low-cost network accessibility to employees, VPN also enables business , research or marketing partners to use secured connections to networks outside the enterprise .

There are many possible options for installing VPNs which are based on the different types of architectures that are associated with them .Trying to avoid using technicalities , we will focus on the basic elements that each type of VPN Architecture is associated with , although some topics are analytically described . There are nine types of architectures that are basically examined in our report. They are NSP-supplied VPNs , Firewall-based VPNs , Black-box-based VPNs , Router-based VPNs , Remote Access-based VPNs , Application-aware VPNs , Multiservice VPNs & Tunnel Swithes-based VPNs and Software-based VPNs .

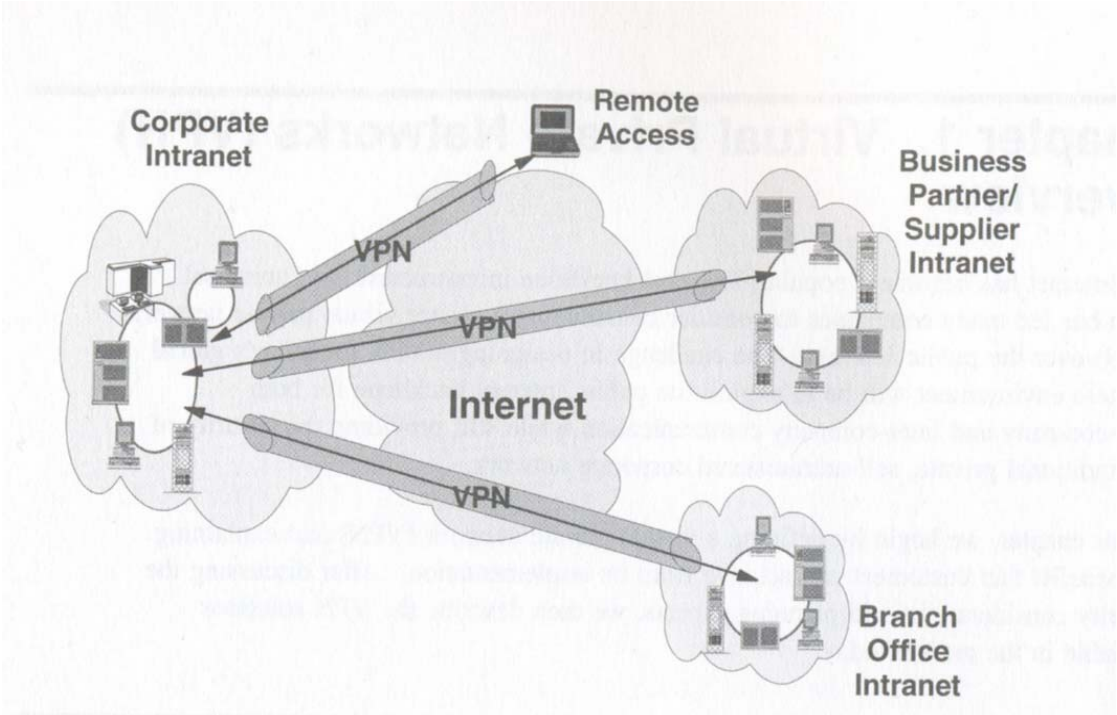
ΠΕΡΙΛΗΨΗ

Σύμφωνα με ένα ευρέως αποδεκτό ορισμό που δόθηκε από το κυβερνητικό ινστιτούτο πληροφορικής , τα Εικονικά Ιδιωτικά Δίκτυα προσδιορίζονται ως ένα δίκτυο που συντίθεται από εικονικά κυκλώματα , εντός του οποίου κυκλοφορούν ιδιωτικές πληροφορίες (public traffic) δια μέσω δημοσίων ή διαμοιραζόμενων δικτύων όπως το Διαδίκτυο ή τα δίκτυα που υποστηρίζουν οι διάφοροι παροχείς δικτυακών υπηρεσιών (NSPs) . Συχνά στη βιβλιογραφία των VPNs συναντώνται οι όροι " tunnel" ή "tunneling" καθώς πίσω από αυτούς εμπεριέχεται η γενικότερη φιλοσοφία πάνω στην οποία στηρίζεται η λειτουργία των VPNs . Ειδικότερα , ο όρος "tunneling" αναφέρεται στο μηχανισμό ενθυλάκωσης (encapsulating) ενός τύπου πακέτου πληροφορίας εντός ενός διαφορετικού τύπου πακέτου κατά τέτοιο τρόπο ώστε να επιτυγχάνεται η ασφαλής κυκλοφορία δεδομένων ανάμεσα στα διάφορα δικτυακά μονοπάτια μετάδοσης (paths) .

Σε γενικές γραμμές μια εταιρία θα πρέπει να αποφασίσει ως προς το ποιό είναι το κατάλληλο μοντέλο VPN σύμφωνα με τους στόχους που έχει θέσει και την στατηγική της , παρ` ολαυτά υπάρχουν τρία μοντέλα VPN που συνήθως επιλέγονται σύμφωνα με τις συνήθεις επιλογές που έχουν κάνει στο παρελθόν τόσο Αμερικανικές όσο και Ευρωπαϊκοί οργανισμοί . Συγκεκριμένα τα τρία αυτά μοντέλα Εικονικών Ιδιωτικών Δικτύων είναι τα Pure Provider Model , Hybrid Provider Model και toEnd-to-End Model .

Στις περισσότερες περιπτώσεις τα εικονικά δίκτυα αναλαμβάνουν το ρόλο ενός λογικού δικτύου που χρησιμεύει στην επικοινωνία ανάμεσα σε γεωγραφικά απομακρυσμένους οργανισμούς . Επίσης επιτρέπουν στους κινητούς υπαλλήλους (mobile employees) να έχουν πρόσβαση στο εσωτερικό δίκτυο (intranet) της εταιρίας τους διαμέσω διαδικτυακών ασφαλών συνδέσεων .Για τη επίτευξη του σκοπού αυτού συνδυάζονται παράλληλα με τα VPNs διάφορες συνδέσεις τύπου dial-up, ασύρματες όπως και συνδέσεις ευρείας ζώνης (broadband) από ISPs .

Οι διάφοροι τύποι VPN που συναντώνται στηρίζονται στις διαφορετικές αρχιτεκτονικές εγκατάστασης που επιλέγονται κάθε φορά . Στη παρούσα εργασία καταβάλλεται προσπάθεια θεωρητικής προσέγγισης των διαφόρων αρχιτεκτονικών που χρησιμοποιούνται στα VPNs χωρίς αναφέρονται εξειδικευμένες πληροφορίες που σχετίζονται με μηχανολογικά θέματα .Οι εννέα διαφορετικές αρχιτεκτονικές VPN που εξετάζονται είναι οι ακόλουθες : α) NSP-supplied VPNs , β) Firewall-based VPNs , γ) Black-box-based VPNs , δ) Router-based VPNs , ε) Remote Access-based VPNs , στ) Application-aware VPNs , ζ) Multiservice VPNs και Tunnel Switches-based VPNs , η) Software-based VPNs .



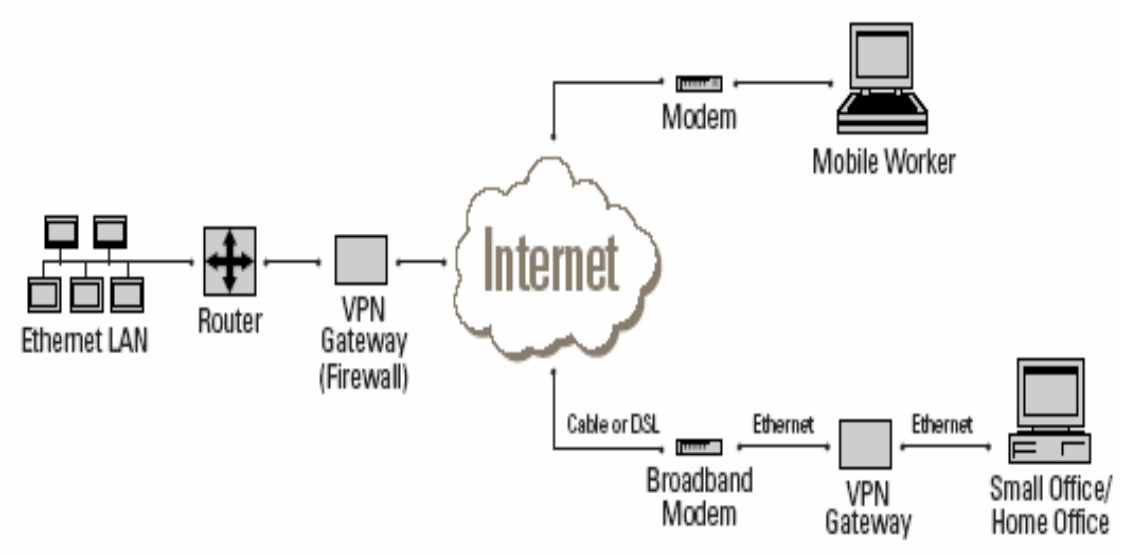
1 . ΠΡΟΛΟΓΟΣ

Η ραγδαία εξάπλωση του Διαδικτύου την τελευταία κυρίως δεκαετία έχει επιφέρει εντελώς καινούργιους τρόπους επικοινωνίας από τους καθιερωμένους . Επιχειρήσεις , οργανισμοί και απλοί άνθρωποι μπορούν πλέον να επικοινωνούν, να ανταλλάσσουν πληροφορίες και να συνδιαλέγονται ανεξάρτητα από γεωγραφικές αποστάσεις. Στις μέρες μας το Διαδίκτυο θεωρείται το ιδανικό μέσο για ανταλλαγή και ανάκτηση δεδομένων εξαιτίας του χαμηλού κόστους σύνδεσης .

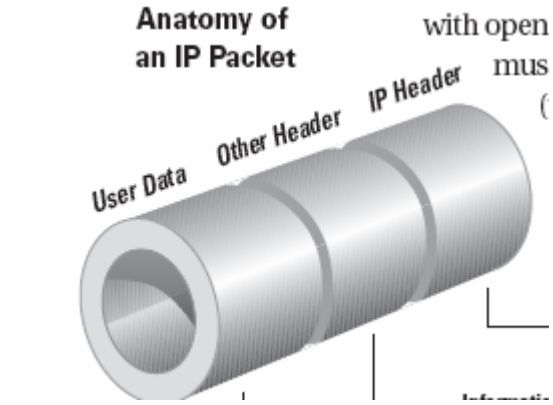
Καθώς όμως το Διαδίκτυο αποτελεί ένα κοινώς διαμοιραζόμενο μέσο που προκύπτει από την σύνδεση εκατοντάδων δικτύων έτσι ώστε εκατομμύρια χρηστών να μπορούν να συνδεθούν σ` αυτό , αυξήθηκε όλο και περισσότερο και η ανασφάλεια για το κατά πόσο διατηρείται το απόρρητο ευαίσθητων πληροφοριών . Τα πολλά κρούσματα ηλεκτρονικού εγκλήματος που παρατηρήθηκαν αύξησαν ακόμη περισσότερο το φόβο των επιχειρήσεων να συνδιαλλαγούν ηλεκτρονικά .

Η αρχική αδυναμία των πρωτοκόλλων του Διαδικτύου να ικανοποιήσουν την υψηλή ασφάλεια δεδομένων αλλά και η αυξανόμενη ανάγκη επέκτασης της επιχειρησιακής δραστηριότητας σχεδόν όλων των σύγχρονων εταιριών σε διακρατικό επίπεδο συνετέλεσαν στην πραγματοποίηση επιστημονικών ερευνών στα πλαίσια προσπάθειας για την αύξηση της αξιοπιστίας του Internet . Ένας από τους καρπούς των ερευνών αυτών υπήρξαν τα Εικονικά Ιδιωτικά Δίκτυα (VPNs) που ουσιαστικά εξασφαλίζουν την εικονική δικτύωση επιχειρήσεων με υψηλή αξιοπιστία και χαμηλό κόστος . Σύμφωνα με τη φιλοσοφία δημιουργίας των Εικονικών Ιδιωτικών Δικτύων καθίσταται εφικτή η ασφαλής επικοινωνία γεωγραφικά απομακρυσμένων Intranets ή γενικότερα ιδιωτικών δικτύων μέσα από τη σύνδεση των επιρρεπών ,ως προς την ασφάλεια δεδομένων , δημόσιων δικτύων που συνθέτουν το Διαδίκτυο .

Πριν προχωρήσουμε όμως στην ανάλυση των χαρακτηριστικών και αρχιτεκτονικών των VPNs θα ήταν χρήσιμο, σύμφωνα και με την παρακάτω εικόνα, να παρουσιαστεί με γενικά λόγια πώς λειτουργεί και από τι απαρτίζεται κάποιο Εικονικό Ιδιωτικό Δίκτυο .Καταρχήν κάποιος κύριος υπολογιστής (host) αποστέλλει δεδομένα σε μια συσκευή VPN , η οποία βρίσκεται τοποθετημένη στο σημείο εκείνο όπου πραγματοποιείται η επικοινωνία του ιδιωτικού δικτύου μιας π.χ. εταιρίας με το δημόσιο δίκτυο . Κατόπιν η συσκευή VPN επεξεργάζεται τα δεδομένα που παρέλαβε και ερευνά εάν έχουν διαμορφωθεί σύμφωνα με τους κανόνες ασφαλείας που επιβάλλει ο διαχειριστής δικτύου .Στη συνέχεια καθιστά ασφαλή τα δεδομένα μέσω κάποιων αλγορίθμων ή τα αφήνει ανέπαφα εάν κριθεί ότι είναι ήδη ασφαλή .



Όταν κριθεί απαραίτητη η ασφάλεια των δεδομένων , η συσκευή VPN ``αποφασίζει`` να κρυπτογραφήσει την πληροφορία επικολλώντας κάποια ψηφιακή υπογραφή πάνω στο πακέτο δεδομένων που πρόκειται να αποσταλεί όπως επίσης και τις IP διευθύνσεις του αποστολέα αλλά και του παραλήπτη host υπολογιστή .



Στη συνέχεια η συσκευή VPN επικολλά μια νέα επικεφαλίδα (ψηφιακή υπογραφή) πάνω στα δεδομένα η οποία περιέχει πληροφορίες για την συσκευή παραλήπτη από την άλλη μεριά του δικτύου για το πώς εκείνη θα διαχειριστεί τις μεθόδους προστασίας των δεδομένων .Μετά από τη διαδικασία αυτή , η VPN συσκευή ενθυλακώνει (encapsulates) το κρυπτογραφημένο πακέτο πληροφορίας με τις IP διευθύνσεις της αντίστοιχης συσκευής ή συσκευών-παραλήπτη .Έτσι δημιουργείται το ιδιωτικό tunnel [1] εντός του οποίου μεταδίδονται τα ασφαλή δεδομένα διαμέσω του δημοσίου δικτύου . Κατά το τελικό στάδιο , μόλις το πακέτο πληροφορίας προσεγγίσει τη συσκευή παραλήπτη πραγματοποιείται εκεί η αντίστροφη διαδικασία της ενθυλάκωσης (decapsulation) , η ψηφιακή υπογραφή εξετάζεται και τελικά το πακέτο αποκρυπτογραφείται .

Η εμφάνιση των Εικονικών Ιδιωτικών Δικτύων υπήρξε αρκετά επιδραστική στον χώρο της διασύνδεσης των επιχειρήσεων καθώς ,όπως θα δούμε και στην ενότητα 3 , οι παραδοσιακές τακτικές δικτύωσης (μισθωμένες γραμμές , frame relay κ.τ.λ.) καθίστανται πλέον αντιοικονομικές αλλά και ανεπαρκείς ως προς την αξιοπιστία που παρέχουν σε σχέση με το υψηλό κόστος που απαιτούν . Τα Εικονικά Ιδιωτικά Δίκτυα φαίνεται ότι θα συνεχίζουν αν απασχολούν ολοένα και περισσότερο την κοινωνία της επιστήμης της πληροφορικής εξαιτίας της υψηλής ασφάλειας που παρέχουν αναλογικά με το χαμηλό κόστος εγκατάστασης τους

[1] Για τα tunnels θα μιλήσουμε πιο αναλυτικά στις επόμενες ενότητες .

2. ΤΑ ΤΡΙΑ ΜΟΝΤΕΛΑ VPN

Όπως προαναφέρθηκε και στον πρόλογο ο τύπος των Εικονικών Ιδιωτικών Δικτύων που φαίνεται να δεσπόζει στην αγορά είναι εκείνα που βασίζονται στην τεχνολογία και στην αρχιτεκτονική του Διαδικτύου . Η αρχιτεκτονική αυτή χαρακτηρίζεται ως ανοιχτή και ταυτόχρονα διαμοιραζόμενη καθώς κατ` αυτόν τον τρόπο επιτυγχάνεται η επικοινωνία των εκατοντάδων διαφορετικών και ασύμβατων δικτύων ανά την υφήλιο που διαφορετικά δεν θα ήταν επιτρεπτή .Πριν όμως αναλυθούν οι διάφορες αρχιτεκτονικές των Εικονικών Ιδιωτικών Δικτύων καλό θα ήταν να αναφερθούν τα χαρακτηριστικά των γενικών μοντέλων VPNs , συμπεριλαμβανομένων και των αρχιτεκτονικών που δεν στηρίζονται στην ``ανοιχτή`` αρχιτεκτονική του Διαδικτύου .

Υπάρχουν τρία κυρίως ευρέως διαδεδομένα μοντέλα VPNs και οι κύριες διαφορές τους στηρίζονται καταρχήν στην τοποθεσία τόσο των δυο άκρων του δικτύου (service end points) όσο και στην τοποθεσία των δυο άκρων του tunnel . Ένα άλλο κριτήριο διαφοράς αποτελεί των τριών μοντέλων VPNs και το κατά πόσο υψηλό θα είναι το επίπεδο διαχείρισης του δικτύου (level of management) που απαιτείται . Επίσης τα μοντέλα VPNs διακρίνονται με βάση την ποιότητα της υπηρεσίας που παρέχουν (QoS) αλλά και ως προς τον βαθμό εμπιστοσύνης που μπορεί να αποδοθεί πάνω στον παροχέα υπηρεσιών (NSP) .

Σύμφωνα με το πρώτο μοντέλο VPN που χαρακτηρίζεται ως αμιγώς στηριζόμενο στον παροχέα υπηρεσιών (Pure Provider Model) , το μεγαλύτερο μέρος των διεργασιών που απαιτούνται για την ομαλή λειτουργία του εικονικού δικτύου επωμίζεται ο παροχέας δικτυακών υπηρεσιών και όχι η αρχιτεκτονική δομή του επιχειρησιακού δικτύου .Κατά το μοντέλο αυτό συνήθως αναφέρεται μόνο ένα δίκτυο του NPS , ενώ υπάρχει αυστηρή διάκριση ανάμεσα στο δίκτυο του οργανισμού ή

της επιχείρησης και στο δίκτυο του παροχέα δικτυακών υπηρεσιών . Η απομακρυσμένη πρόσβαση στο επιχειρησιακό δίκτυο συνήθως πραγματώνεται μέσω αφιερωμένων κυκλωμάτων όπως οι συνδέσεις τύπου T1 και T3 . Άλλοτε πάλι χρησιμοποιούνται για τον ίδιο σκοπό συνδέσεις Ασύγχρονης Μετάδοσης Δεδομένων (ATM) ή συνδέσεις Αναμετάδοσης Πλαισίου (Frame Relay) .

Ο πελάτης ή η επιχείρηση κατέχει αλλά και διαχειρίζεται τον εξοπλισμό αλλά και το λογισμικό (software) που απαιτεί το απομακρυσμένης πρόσβασης Εικονικό Ιδιωτικό Δίκτυο , ενώ τον εξοπλισμό και το λογισμικό που απαιτούνται εντός του δικτύου του NSP διαχειρίζεται ο ίδιος ο παροχέας υπηρεσιών . Στο Pure Provider μοντέλο ο παροχέας υπηρεσιών εγκαθιστά VPN-tunnels από τη μια άκρη έως την άλλη (edge-to-edge) του δικτύου χρησιμοποιώντας τα ιδιωτικά κυκλώματα και στις δυο άκρες του δικτύου για να επιτύχει την ασφαλή μετάδοση των δεδομένων .Εν τέλει ο παροχέας δικτυακών υπηρεσιών ελέγχει σε μεγάλο βαθμό την όλη λειτουργία του VPN αποκαθιστώντας τα τυχόν προβλήματα που μπορούν να προκύψουν κατά την επικοινωνία των δυο άκρων (ends) του VPN .

Σύμφωνα με δεύτερο μοντέλο VPN που χαρακτηρίζεται ως Υβριδικά Εξαρτώμενο από τον παροχέα των δικτυακών υπηρεσιών (Hybrid Provider Model) τόσο το εσωτερικό δίκτυο της επιχείρησης όσο και το δίκτυο του NSP επωμίζεται τον έλεγχο των διεργασιών που απαιτούνται για την ομαλή λειτουργία του εικονικού ιδιωτικού δικτύου . Ένα VPN tunnel αρχικοποιείται εντός του δικτύου του παροχέα υπηρεσιών ενώ ολοκληρώνεται εντός του δικτύου του οργανισμού.

Σύμφωνα με αυτό το μοντέλο ο παροχέας δικτυακών υπηρεσιών είναι υπεύθυνος για την αρχικοποίηση των VPN tunnels για λογαριασμό των απομακρυσμένων χρηστών (remote users) του δικτύου , μόλις επιβεβαιωθεί η εγκυρότητα της ταυτότητας των χρηστών (users authentication) . Μόλις λοιπόν οι απομακρυσμένοι χρήστες συνδεθούν με το δίκτυο του οργανισμού μπορεί να επαναληφθεί η διαδικασία πιστοποίησης της ταυτότητας τους προτού να αποκτήσουν πρόσβαση στα δεδομένα του οργανισμού . Μόλις δηλαδή πιστοποιηθεί η ταυτότητα των χρηστών μπορούν εκείνοι στη συνέχεια να αποκτήσουν πρόσβαση σε όλες τις παρεχόμενες υπηρεσίες του δικτύου κατά παρόμοιο τρόπο όπως θα γινόταν και στην περίπτωση σύνδεσης τους με το τοπικό δίκτυο (LAN) της εταιρίας τους .

Τέλος σύμφωνα με το τρίτο μοντέλο VPN που χαρακτηρίζεται Από Άκρη Έως Άκρη (end-to-end) ο παροχέας δικτυακών υπηρεσιών λειτουργεί μόνο ως μεταφορικό μέσο των δεδομένων που μεταδίδονται εντός του Εικονικού Ιδιωτικού Δικτύου . Οι δυο άκρες του δικτύου , τόσο αυτές του παροχέα όσο και αυτές του tunnel , μπορεί να είναι κάποιος επιτραπέζιος υπολογιστής ή κάποια συσκευή VPN που μπορεί να λειτουργήσει ως ``διαχειριστής `` (proxy) για πολλαπλούς επιτραπέζιους υπολογιστές . Θα πρέπει τέλος να σημειωθεί ότι και οι δυο άκρες του δικτύου βρίσκονται εκτός του δικτύου που διαχειρίζεται ο παροχέας δικτυακών υπηρεσιών .

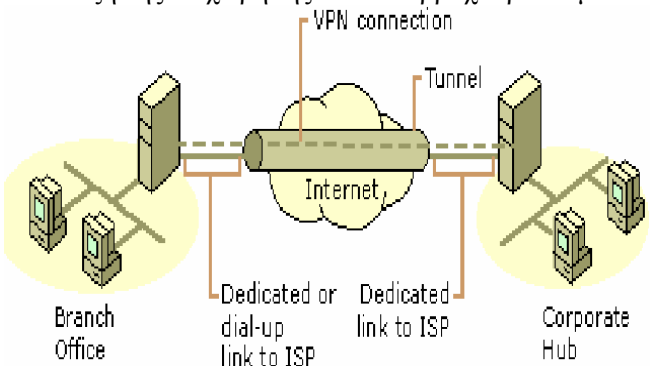
Με βάση λοιπόν τα τρία αυτά μοντέλα VPN δηλαδή το Αμιγώς Εξαρτώμενο από τον NSP , το Υβριδικό μοντέλο και το από Άκρη Έως Άκρη μοντέλο απορρέουν οι ειδικές κατηγορίες αρχιτεκτονικών των εικονικών Ιδιωτικών Δικτύων που θα αναλυθούν στην ενότητα 5 . Κρίνεται όμως χρήσιμο αυτό να αναλυθούν περισσότερο τα VPN που βασίζονται στην αρχιτεκτονική του Διαδικτύου και να περιγραφούν τα πλεονεκτήματα τους έναντι των αρχικών αρχιτεκτονικών VPN ώστε να κατανοηθεί η μεγάλη εξάπλωση των διαδικτυακών εικονικών δικτύων

Σημείωση :

Σε κάθε ενότητα θα παρατίθενται και σχετικά e-links από το Διαδίκτυο όπου αντλήθηκαν σημαντικές πληροφορίες για την ανάλυση του θέματος της εργασίας .

3 . ΤΑ INTERNET-BASED VPN ΚΑΙ ΤΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥΣ

Μια σύγχρονη επιχείρηση πρέπει να υποστηρίζει πολλών τύπων δικτυακές συνδέσεις έτσι ώστε να μπορεί να είναι ανταγωνιστική εντός του σύγχρονου οικονομικού περιβάλλοντος , όπου η υψηλή ταχύτητα απορρόφησης και ανάκτησης της πληροφορίας παίζουν καθοριστικό ρόλο για την ανάπτυξη της επιχείρησης τόσο σε βραχυπρόθεσμο όσο και σε μεσοπρόθεσμο χρονικό ορίζοντα .



Συγκεκριμένα οι υπάλληλοι θα πρέπει να έχουν πρόσβαση στα δεδομένα που μεταδίδονται εντός του επιχειρησιακού τους ιδιωτικού εσωτερικού δικτύου (intranet) όταν ταξιδεύουν , επίσης θα πρέπει να έχουν την δυνατότητα να τηλεσυνδιαλέγονται από απομακρυσμένες περιοχές εκτός του χώρου της δουλειάς . Παράλληλα οι επιχειρησιακοί συνεργάτες ενός οργανισμού θα πρέπει να μπορούν να επικοινωνούν και να συνδιαλέγονται διαμέσω εξωτερικών ιδιωτικών δικτύων (extranets)
τόσο σε βραχυπρόθεσμο επίπεδο όσο και σε μακροπρόθεσμο στρατηγικό επίπεδο .

Ταυτόχρονα ολοένα και αποδεικνύεται η ανεπάρκεια των αρχικών αρχιτεκτονικών των δικτύων ευρείας κλίμακας (WAN) που υποστήριζαν τη επικοινωνία του επιχειρησιακού δικτύου με τα απομακρυσμένα γραφεία της (branch offices) . Αυτό οφείλεται στο γεγονός ότι οι πρωταρχικές συνδέσεις τύπου μισθωμένων γραμμών ή αναμετάδοσης πλαισίου δεν είναι ευέλικτες ως προς την ικανότητα γρήγορης εγκατάστασης συνδέσεων άλλα και τηλεσυνδιάσκεψης .

Από την άλλη μεριά , τα VPN που βασίζονται στο Διαδίκτυο εκτός από την χαμηλότερο κόστος σύνδεσης που απαιτούν μπορούν να προσφέρουν ταυτόχρονα και άλλα πλεονεκτήματα που έμμεσα ωφελούν την επιχείρηση . Πρώτα από όλα ένα παραδοσιακό ιδιωτικό δίκτυο που βασίζεται είτε σε συνδέσεις τύπου T1 (1,5 Mbps) είτε T3 (45 Mbps) αμέσως επιβαρύνεται με στάνταρ έξοδα που έχουν να κάνουν με το κόστος εγκατάστασης του δικτύου , το μηνιαίο τέλος , το κόστος επιβάρυνσης εξαιτίας της χιλιομετρικής αποστάσεως όπως επίσης και τα επιπρόσθετα μηνιαία έξοδα που απαιτούνται για συνδέσεις σε μεγαλύτερο εύρος μετάδοσης από το συνηθισμένο . Τα διαδικτυακά όμως VPN δεν επιβαρύνονται με τα παραπάνω κόστη καθώς βασίζονται στη φιλοσοφία της ανοικτής δομής (open infrastructure) του Διαδικτύου .

Επίσης η επιχείρηση που χρησιμοποιεί ένα Εικονικό Ιδιωτικό Δίκτυο δεν απαιτείται πλέον να υποστηρίζει αλλά και να συντηρεί τις συνδέσεις από σημείο σε σημείο (point-to-point) συμπεριλαμβανομένου και του κόστους συντήρησης των δικτυακών modems αλλά και των άλλων δικτυακών συσκευών που αυτές οι συνδέσεις συνεπάγονται .Έτσι το τμήμα πληροφοριακής τεχνολογίας της επιχείρησης μπορεί να μειώσει το κόστος συντήρησης του δικτύου καθώς αντικαθίστανται πλέον τα modems και τα πολλαπλά κυκλώματα αναμετάδοσης πλαισίου από μια μοναδική σύνδεση ευρείας κλίμακας που μπορεί να μεταδώσει ταυτόχρονα δεδομένα από κάποιο απομακρυσμένο χρήστη , μεταξύ δυο τοπικής κλίμακας δικτύων (LAN-to-LAN) αλλά και διαμέσω του Διαδικτύου .

Τέλος θα πρέπει να επισημανθεί ότι η χρησιμοποίηση των διαδικτυακών VPNs εξοικονομεί πόρους και για το λόγο ότι δεν απαιτείται να γίνεται πλέον όλη η τεχνική υποστήριξη του δικτύου από την ίδια την επιχείρηση καθώς οι παροχείς διαδικτυακών υπηρεσιών αναλαμβάνουν το μεγαλύτερο μέρος της υποστήριξης του VPN .

- \Find VPN (Virtual Private Networks) The Advantages of a VPN.htm
- \Find VPN (Virtual Private Networks) What About VPN Security.htm
- \Find VPN (Virtual Private Networks) What is VoIP __ Explain.htm

- \HNS Review - MPLS and VPN Architectures, CCIP Edition.htm(SEARCH MACHINE)---REVIEW OF A BOOK"MPLS & VPN ARCHITECTURES" BY BERISLAV KUCAN

- \IS Auditing Guideline Review of Virtual Private Networks.htm---A review on vpn by Information Systems Audit and Control Association

- \Logtel Seminar New Technologies in IP Networking.htm--- e-seminar by Logtel computer communication group

- \Pearson Books - MPLS and VPN Architectures.htm----review of book"MPLS and VPN Architectures
  Ivan Pepelnjak, Jim Guichard

- \TISC 2001 Seminars.htm---overview on vpn by The Internet Security Conference

- \v2.htm--- white paper on IPSec

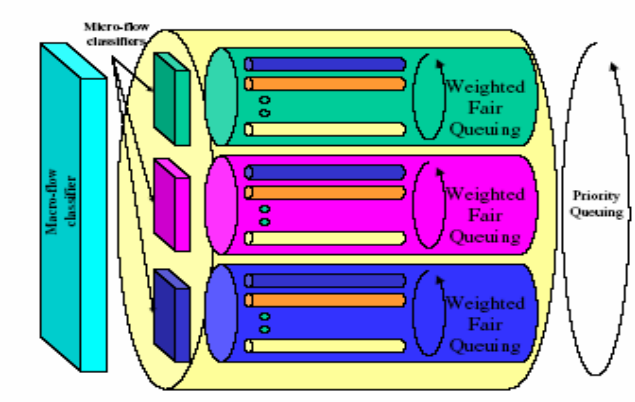
- \v4.htm----IPSec Virtual Private Networks: Conformance and Performance Testing

4. TUNNELING & ΤΑ ΠΡΩΤΟΚΟΛΛΑ ΤΩΝ VPNs

Κατά την παρουσίαση των διαφόρων αρχιτεκτονικών VPN που θα ακολουθήσει στην ενότητα 5 δεν αναφέρονται με λεπτομέρεια οι διάφορες τεχνικές διεργασίες αλλά και ο τρόπος λειτουργίας των διαφόρων πρωτοκόλλων δικτύου που σχετίζονται με κάθε αρχιτεκτονική καθώς δεν αποτελεί αντικείμενο της παρούσας εργασίας η παράθεση εξειδικευμένων εννοιών . Ωστόσο θα πρέπει να περιγράφούν με γενικά λόγια τόσο ο μηχανισμός tunneling όσο και τα πιο διαδεδομένα πρωτόκολλα VPN ώστε να γίνει πιο εύκολα η κατανόηση των διαφόρων αρχιτεκτονικών .

4.1 TUNNELING

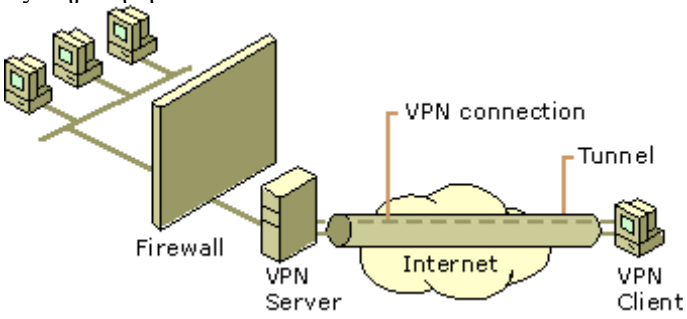
Όπως υπονοείται και από τον ορισμό των Εικονικών Ιδιωτικών Δικτύων αναφερόμαστε σε εικονικές συνδέσεις ή αλλιώς λογικές οι οποίες εγκαθίστανται ανεξάρτητα από τη φυσική δομή και τα χαρακτηριστικά του δικτύου που τις περισσότερες φορές είναι το Διαδίκτυο . Αντίθετα από τις μισθωμένες γραμμές , οι εικονικές συνδέσεις των VPNs δημιουργούνται μόλις υπάρξει η ανάγκη για αυτό και διακόπτονται αμέσως όταν οι συνδέσεις πλέον δεν απαιτούνται .



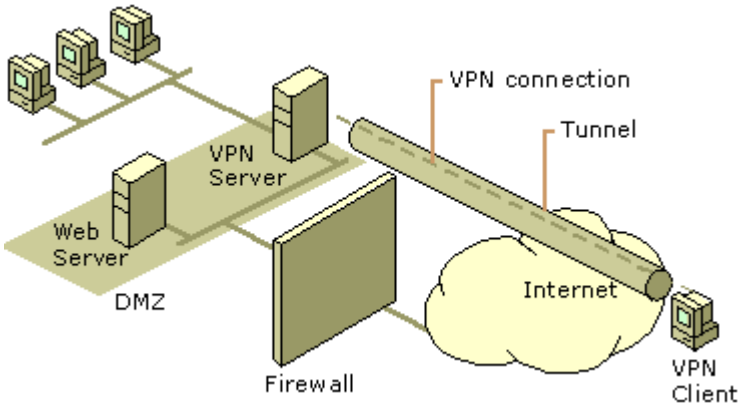
Η παραπάνω φιλοσοφία λειτουργίας στηρίζεται στη δημιουργία των tunnels κάθε φορά που πραγματοποιείται μια εικονική σύνδεση .Όπως προαναφέρθηκε και στην περίληψη με τον όρο `` tunneling`` αναφερόμαστε στην ενθυλάκωση και κρυπτογράφηση ολόκληρων των μεταδιδόμενων πακέτων πληροφορίας , κατά τέτοιο τρόπο ώστε να αποκρύπτονται από τις δικτυακές εφαρμογές όλα εκείνα τα δεδομένα που αφορούν πληροφορίες σχετικά με τη δομή του δικτύου όπως π.χ. η δρομολόγηση των πακέτων .

Στις δυο άκρες (ends) ενός tunnel μπορεί να βρίσκεται είτε ένας απλός υπολογιστής ή ένα δίκτυο τοπικής κλίμακας (LAN) που συνοδεύεται από κάποια πύλη ασφαλείας (security gateway) . Ένας από τους πιο γνωστούς συνδυασμούς end points ενός tunnel είναι αυτός του απλού υπολογιστή ή πελάτη-με-δίκτο LAN (client-to-LAN) και δημιουργείται κάθε φορά που ένας απομακρυσμένος χρήστης θέλει να συνδεθεί με το δίκτυο της εταιρίας του . Στην προκειμένη περίπτωση η εφαρμογή του χρήστη (client software) προσπαθεί να επικοινωνήσει με την πύλη ασφαλείας που προστατεύει το δίκτυο LAN από την άλλη μεριά του tunnel .

Όπως φαίνεται και στις παρακάτω εικόνες υπάρχουν συνήθως σχεδιασμοί επικοινωνίας της εφαρμογής με την πύλη ασφαλείας .Σύμφωνα με τον πρώτο σχεδιασμό ο client επικοινωνεί πρώτα με κάποιο εξυπηρετητή VPN και διαμέσω αυτού με την πύλη ασφαλείας του LAN , ενώ κατά τον δεύτερο σχεδιασμό ο client επικοινωνεί πρώτα με την πύλη ασφαλείας και στη συνέχεια με κάποιο εξυπηρετητή VPN .



Ο δεύτερος πιο γνωστός συνδυασμός end points του tunnel αναφέρεται στην επικοινωνία δυο δικτύων τοπικής κλίμακας (LAN-to-LAN) . Στην περίπτωση αυτή υπάρχει πύλη ασφαλείας και στις δυο άκρες του tunnel και η καθεμιά παίζει το πόλο του περιβάλλοντος διασύνδεσης του tunnel με το κάθε LAN .



4. 2 ΤΑ ΠΡΩΤΟΚΟΛΛΑ

Παρόλο που χρησιμοποιείται μια μεγάλη ποικιλία από πρωτόκολλα θα αναφερθούμε στα πέντε πιο δημοφιλή καθώς τα περισσότερα πρωτόκολλα αποτελούν παραλλαγές αυτών των πέντε και οφείλονται μάλλον στη διαφορετικότητα των υπηρεσιών που προσφέρουν οι διάφοροι οργανισμοί υποστήριξης Εικονικών Ιδιωτικών Δικτύων αλλά και στον διαφορετικό τύπο VPN που ικανοποιεί την κάθε μια επιχείρηση ξεχωριστά .

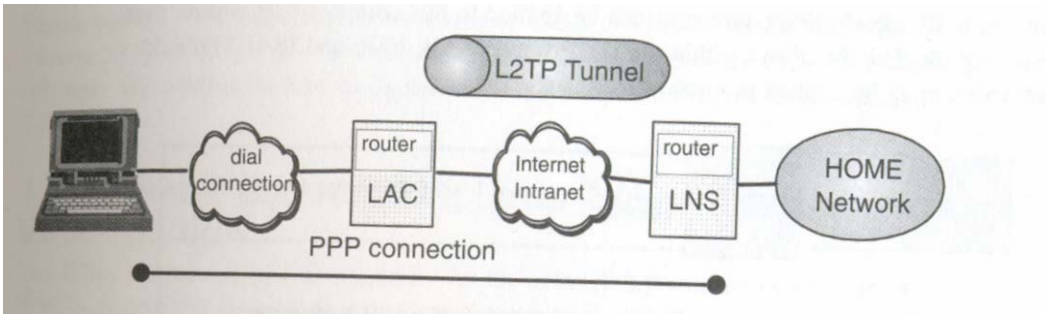
Point-to-Point Tunneling Protocol (PPTP)

Το πρωτόκολλο PPTP αποτελεί ένα από τα πρώτα πρωτόκολλα που αναπτύχθηκαν για να υποστηρίξουν εικονικά Ιδιωτικά Δίκτυα κυρίως τύπου dial-up .Το PPTP βασίζεται πάνω στο γνωστό PPP (από σημείο σε σημείο) πρωτόκολλο που παρέχει απομακρυσμένη πρόσβαση στο Διαδίκτυο δηλαδή το PPTP δημιουργεί tunnels σε περιβάλλον Internet . Είναι αρκετά απλό ως προς την ενθυλάκωση και κρυπτογράφηση των πακέτων πληροφορίας ενώ μπορεί να διαχειριστεί και διαφορετικά πρωτόκολλα από το από το πρωτόκολλα του Διαδικτύου (IP) .

Layer-2-Forwarding Protocol (L2F)

Σε αντίθεση με το PPTP το πρωτόκολλο L2F δεν στηρίζεται στην αρχιτεκτονική του Διαδικτύου οπότε μπορεί να διαχειριστεί και άλλου τύπου συνδέσεις όπως αναμετάδοσης πλαισίου ή ασύγχρονης μετάδοσης δεδομένων . Επίσης το κάθε tunnel μπορεί να υποστηρίξει πάνω από μια συνδέσεις , κάτι που δεν συμβαίνει με PPTP ενώ και το πρωτόκολλο L2F είναι σχεδιασμένο για σύνδεση του απομακρυσμένου χρήστη με το δίκτυο μιας εταιρίας .

Layer -2-Tunneling Protocol (L2TP)



Το πρωτόκολλο αυτό αναπτύχθηκε σε μια προσπάθεια να συνδυαστούν τα πλεονεκτήματα των PPTP και L2F .Μπορεί να υποστηρίξει συνδέσεις τύπου dial-up χρησιμοποιώντας το Διαδίκτυο κατά το μηχανισμό tunneling ενώ κατά την διαμόρφωση των πακέτων πληροφορίας είναι συμβατό και με πακέτα διαφορετικά του περιβάλλοντος του Διαδικτύου όπως αναμετάδοσης πλαισίου ή ασύγχρονης μετάδοσης

IP Security Protocol (IPSec)

Το πρωτόκολλο IPSec αποτελεί ίσως το πιο διαδεδομένο στις διάφορες συνδέσεις εικονικών Ιδιωτικών Δικτύων που ήδη υπάρχουν με διάφορες βέβαια παραλλαγές . Είναι καταρχήν σχεδιασμένο για να εξυπηρετήσει τις ανάγκες υψηλού εύρους ζώνης μετάδοσης που θα υποστηρίζει το Διαδίκτυο δεύτερης γενιάς . Επίσης επιτρέπει στη μια άκρη του tunnel που αποστέλλει δεδομένα , τη δυνατότητα είτε μόνο να πιστοποιήσει (authenticate) είτε μόνο να κρυπτογραφήσει (encrypt) τα πακέτα πληροφορίας όπως επίσης και να εκτελέσει και τις δυο αυτές διεργασίες παράλληλα .

Επειδή το IPSec είναι σχεδιασμένο πάνω στη φιλοσοφία του Internet θεωρείται ως το πιο κατάλληλο για περιβάλλοντα IP σε αντίθεση με τα πρωτόκολλα PPTP και L2TP που ενδείκνυνται για συνδυασμό και διαφορετικών πρωτοκόλλων από το IP του Διαδικτύου .

Multiprotocol Label Switching (MPLS)

Το πρωτόκολλο MPLS έχει σχεδιαστεί με διαφορετική φιλοσοφία από το IPSec καθώς δεν επικεντρώνεται τόσο στη βελτιστοποίηση του μηχανισμού κρυπτογράφησης ενώ είναι συμβατό σε περιβάλλον συνδέσεων τύπου ασύγχρονης μετάδοσης ταυτόχρονα με συνδέσεις IP . Επίσης σε αντίθεση με το IPSec , το πρωτόκολλο MPLS είναι αρχικά σχεδιασμένο με σκοπό υψηλότερη δυνατή ποιότητα υπηρεσιών (QoS) όπως για παράδειγμα τη καλύτερη δυνατή διαχείριση περιπτώσεων συμφόρησης αλλά και λανθασμένης δρομολόγησης .

- \Virtual Private Networking.htm---review on VPN by WINDOWSECURITY.com
- \www.infosyssec.net/infosyssec/secvpn1.htm---- article on Vpn by "theWHIR's" (findvpn)
- \VPN Bibliographies - links and VPN article references.htm---- Te Security Portal for Information System Security Professionals
- \VPN FAQ.htm----- BY ACTIUS SUPPORT vpn faqs

- \ cisco.com--- A Comparison Between MPLs and IPSec (white paper)
- \http://computer.org/internet ---- article " The Latest In Vpn" Part a & Part b
- \ Remote Access Vpn Solutions (overview) By Check Point Software Technologies
- \pdf file by Cisco " How Vpn Works"
- \www.dataconnection.com----------"VPN Technologies-AComparison" (white paper)
- \www.diversinet.com--- white paper-- "Passport Wireless VPN"

5 . ΟΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΤΩΝ VPNs

Η αρχιτεκτονική των Εικονικών Ιδιωτικών Δικτύων που στηρίζεται στο Διαδίκτυο αποτελεί το πλέον σύγχρονο και ταυτόχρονα διαδεδομένο μοντέλο VPN γι ` αυτό και η ανάλυση επικεντρώνεται κυρίως σ` αυτό . Στο σημείο αυτό θα πρέπει να επισημανθεί ο σπουδαίος πόλος που παίζουν οι πύλες ασφαλείας (security gateways) ως ένα από τα βασικά συστατικά ενός Εικονικού Ιδιωτικού Δικτύου . Οι πύλες ασφαλείας τοποθετούνται μεταξύ των δημοσίων και ιδιωτικών δικτύων αναλαμβάνοντας το έργο της προστασίας του ιδιωτικού δικτύου από ανεπιθύμητες μη εξουσιοδοτημένες (unauthorized) συνδέσεις .

Μπορούν επίσης άλλοτε να διενεργούν το μηχανισμό tunneling και άλλοτε να αναλαμβάνουν την κρυπτογράφηση των απόρρητων δεδομένων πριν αυτά μεταδοθούν διαμέσω του δημοσίου δικτύου . Σύμφωνα με τα υπάρχοντα τεχνολογικά δεδομένα στο χώρο των VPN , η πύλη ασφαλείας μπορεί να έχει τη μορφή δρομολογητών (routers) , firewalls , τη μορφή διαφόρων περιφερειακών συσκευών (VPN Hardware) όπως επίσης και τη μορφή λογισμικού VPN (VPN Software) .

Ας περάσουμε όμως στην ανάλυση των διαφόρων αρχιτεκτονικών VPN με πιο ευρύ κριτήριο όμως διάκρισης από αυτό της μορφής που μπορεί να πάρει μια πύλη ασφαλείας .

5.1. ΤΟ Ε. Ι .Δ . ΠΟΥ ΥΠΟΣΤΗΡΙΖΕΤΑΙ ΑΠΟ ΤΟΝ ΠΑΡΟΧΕΑ ΔΙΚΤΥΑΚΩΝ ΥΠΗΡΕΣΙΩΝ (VPN Supplied By NSP)

Η υποστήριξη ενός Εικονικού Ιδιωτικού Δικτύου από τον παροχέα δικτυακών υπηρεσιών αποτελεί ίσως μια από τις πλέον διαδεδομένες στρατηγικές που ακολουθούν πολλές από τις σύγχρονες επιχειρήσεις που στην προσπάθεια τους να εκμεταλλευτούν τις δυνατότητες των VPN ενώ ταυτόχρονα είναι συνδεδεμένες με το Διαδίκτυο .

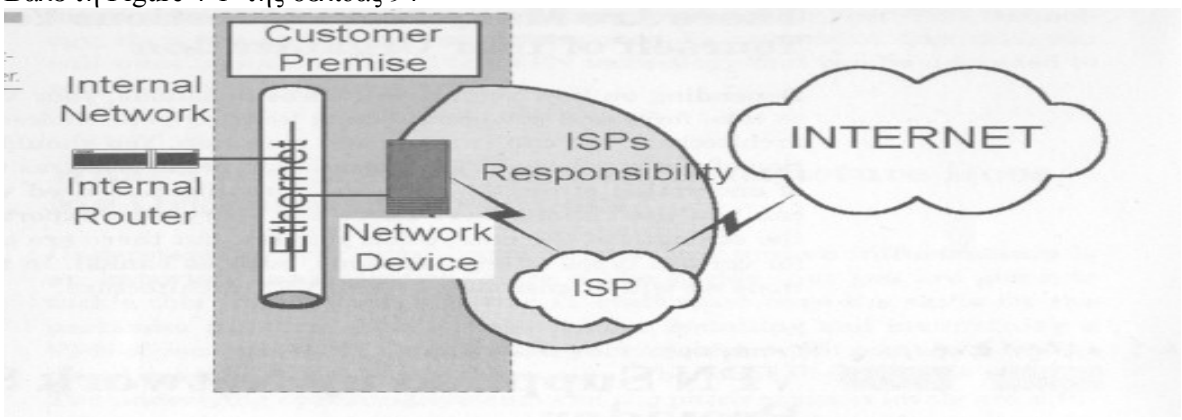
Σύμφωνα με τη συγκεκριμένη αρχιτεκτονική ο παροχέας δικτυακών υπηρεσιών συνήθως (NSP) αναλαμβάνει να εγκαταστήσει κάποια συσκευή VPN για λογαριασμό της επιχείρησης πελάτη η οποία θα δημιουργεί τα tunnels κάθε φορά που θα απαιτείται κάποια εικονική σύνδεση .Τα πακέτα πληροφορίας θα κρυπτογραφούνται από τη συσκευή αυτή όπως επίσης και θα αποκρυπτογραφεί τα αποστελλόμενα πακέτα δεδομένων προς τον υπολογιστή host της επιχείρησης . Αρκετές φορές τοποθετείται κάποιο τοίχος πυρασφάλειας (firewall) ακριβώς μπροστά από τη συσκευή VPN με στόχο τη μεγαλύτερη προστασία των μεταδιδόμενων πληροφοριών

Από τη μια μεριά του firewall συνδέεται ο εσωτερικός δρομολογητής του επιχειρησιακού τοπικού δικτύου ενώ από την άλλη μεριά του firewall συνδέεται ένας εξωτερικός δρομολογητής και ο οποίος με τη σειρά του συνδέεται με τον παροχέα διαδικτυακών υπηρεσιών . Στην εικόνα 5.1. παρουσιάζεται μια μορφή της αρχιτεκτονικής VPN που εξετάζουμε .

Το εικονικό Ιδιωτικό Δίκτυο που υποστηρίζεται από τον παροχέα δικτυακών υπηρεσιών αποτελεί μια καλή επιλογή αρχιτεκτονικής για τους οργανισμούς εκείνους που ενδιαφέρονται κυρίως για την διεξαγωγή τηλεσυνδιασκέψεων (teleconferencing) ή ακόμη θέλουν να επωφεληθούν από τις δυνατότητες της IP τηλεφωνίας , δηλαδή του τηλεφώνου μέσω Διαδικτύου .

Ωστόσο η αρχιτεκτονική αυτή θα μπορούσε να χαρακτηριστεί ως περιορίσιμη ως προς την δυνατότητα αναβάθμισης του Εικονικού Ιδιωτικού Δικτύου με περισσότερες υπηρεσίες καθώς οι NSPs είναι μεγάλοι οργανισμοί που θα πρέπει να υποστηρίζουν μια πληθώρα από VPN συνδέσεις , γεγονός που τους καθιστά δυσκίνητους ως προς την ευκολία αναβάθμισης κάθε φορά που μια επιχείρηση πελάτης ζητά αναβάθμιση του VPN της..

Βάλε τη Figure 4-1 της σελίδας 94



5. 2. ΤΑ ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ ΤΕΙΧΟΣ ΠΥΡΑΣΦΑΛΕΙΑΣ (Firewall – Based VPNs)

Η αρχιτεκτονική του Εικονικού Ιδιωτικού Δικτύου που βασίζεται στο τοίχος πυρασφάλειας είναι μάλλον η πιο διαδεδομένη αυτή τη στιγμή ανάμεσα στις υπόλοιπες και τούτο διότι με την πάροδο των τελευταίων χρόνων το firewall έχει διαδοθεί με τόσο μεγάλους ρυθμούς ώστε θεωρείται πλέον μια καθιερωμένη στρατηγική προστασίας των μεγάλων κυρίως αλλά και των μικρών οργανισμών ενώ είναι ελάχιστες οι επιχειρήσεις που δεν χρησιμοποιούν firewall στο δίκτυο τους .

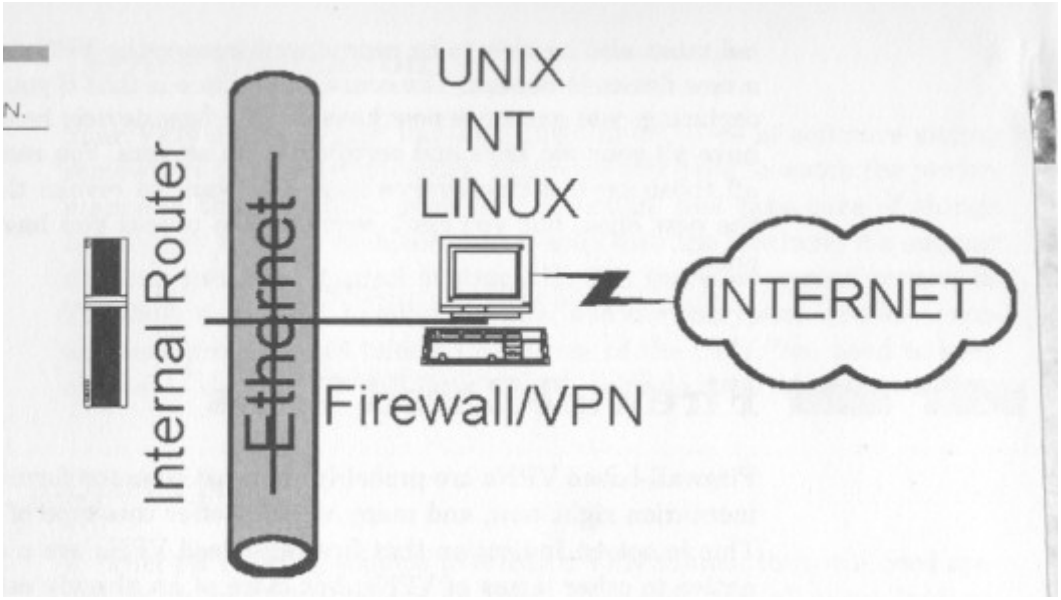
Εφόσον λοιπόν οι πιο πολλές επιχειρήσεις ήδη κατέχουν κάποιας μορφής firewall αυτό που χρειάζονται είναι η υποστήριξη του απαραίτητου λογισμικού κρυπτογράφησης από το ίδιο το firewall. Τις περισσότερες φορές οι ίδιοι οι κατασκευαστές των firewalls προσφέρουν μαζί με το προϊόν και επιπλέον λογισμικό κρυπτογράφησης ανέξοδα ενώ άλλες φορές θα πρέπει η επιχείρηση να επιλέξει εκ των υστέρων ποιο τύπο λογισμικού ανάμεσα στα διαθέσιμα που πωλούν οι κατασκευαστές θα ήταν το κατάλληλο σύμφωνα με τις απαιτήσεις της .

Ένα θετικό χαρακτηριστικό των firewalls είναι η συμβατότητα τους με διάφορες αρχιτεκτονικές δικτύου όπως για παράδειγμα με τοπικά δίκτυα που επικεντρώνονται σε τεχνολογία UNIX , με δίκτυα LAN που βασίζονται σε τεχνολογία NT κ.λ.π.. Ανεξάρτητα όμως από την ευρεία διάδοση των τοίχων πυρασφάλειας και τη μεγάλη τους αποτελεσματικότητα ως προς την ασφάλεια του ενδοεπιχειρησιακού δικτύου , δεν θα πρέπει να θεωρηθούν απόλυτα ασφαλείς , καθώς πρέπει να ταυτόχρονα να σχεδιαστεί και το λειτουργικό σύστημα της μηχανής που διαχειρίζεται το δίκτυο με τον πλέον ασφαλή τρόπο . Προβληματικό και επιρρεπές λειτουργικό σύστημα σε hackers ταυτόχρονα καθιστά προβληματικό και το firewall .

Όπως αναφέρθηκε και στην αρχή πολλοί κατασκευαστές firewalls ενσωματώνουν και δυνατότητες υποστήριξης Εικονικού Ιδιωτικού Δικτύου πάνω στα προϊόντα τους . Τα firewalls διαχειρίζεται ολόκληρη την κυκλοφορία των IP πακέτων και επιτρέπουν ή απορρίπτουν την πρόσβαση δεδομένων προς το δίκτυο ανάλογα με τα φίλτρα προστασίας που υποστηρίζουν .

Τέλος θα πρέπει να σημειωθεί ότι τα firewall που υποστηρίζουν το μηχανισμό tunneling από ενδείκνυνται για μεγάλα δίκτυα ενώ η υποστήριξη τόσο του tunneling όσο και του μηχανισμού

κρυπτογράφησης είναι πιο κατάλληλη για μικρά δίκτυα (1-2 Mbps WANs) όπου δεν υπάρχει υψηλή κίνηση πληροφορίας και δεν απαιτούν συχνή αναβάθμιση .



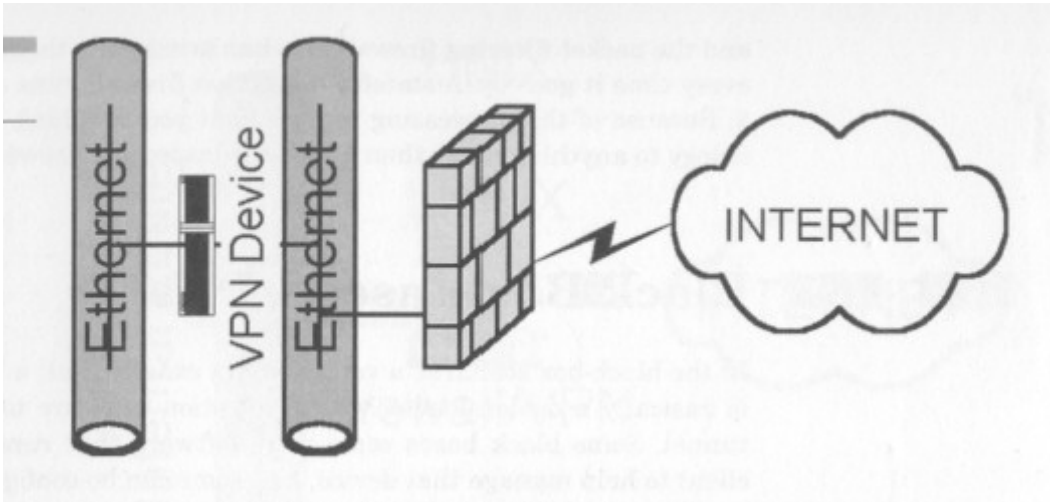
5. 3. ΤΑ ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ BLACK-BOX (Black-Box & Hardware Based VPNs)

Σύμφωνα με την αρχιτεκτονική αυτή των VPNs η επιχείρηση μπορεί να προμηθευτεί από κάποιον κατασκευαστή μια συσκευή δικτύου που συνήθως ονομάζεται black-box και η οποία αναλαμβάνει να δημιουργήσει tunnels εικονικού δικτύου βάσει του λογισμικού κρυπτογράφησης που είναι αποθηκευμένο επάνω στο ίδιο το black-box . Τις περισσότερες φορές η διαχείριση των black-box μπορεί να γίνει από κάποιο επιτραπέζιο υπολογιστή client δεδομένου του αντίστοιχου λογισμικού υποστήριξης . Σε άλλες περιπτώσεις κάποιος browser μπορεί να διαχειρίζεται τα black-box διαμέσω του δικτύου .

Θετικό στοιχείο της αρχιτεκτονικής των black-box συσκευών είναι ότι παρουσιάζουν συμβατότητα με όλα τα πρωτόκολλα που διενεργούν το μηχανισμό tunneling , ωστόσο από την άλλη μεριά πρέπει να σημειωθεί ότι θα πρέπει οι επιχειρήσεις να εγκαταστήσουν κάποιο ξεχωριστό τοίχος πυρασφάλειας αν και τα τελευταία χρόνια άρχισαν να διατίθενται στην αγορά και συσκευές black-box που ενσωμάτωναν και τις δυνατότητες ενός firewall .

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι υπάρχουν στην αγορά αρχιτεκτονικές VPN που είναι παρόμοιες με τον τρόπο λειτουργίας μιας συσκευής black-box , γι` αυτό θα τις ονομάσουμε αρχιτεκτονικές τύπου Hardware . Οι περισσότερες λοιπόν από αυτές τις περιφερειακές συσκευές εικονικού δικτύου συνήθως λειτουργούν ως γέφυρες (Bridges) που αναλαμβάνουν την κρυπτογράφηση και τοποθετούνται μεταξύ των δρομολογητών του δικτύου και των συνδέσεων με δίκτυα ευρείας κλίμακας .

Αν και τις περισσότερες φορές οι συσκευές αυτές σχεδιάζονται ώστε να υποστηρίξουν ένα εικονικό ιδιωτικό δίκτυο όπου και στις δυο άκρες του βρίσκονται δίκτυα τοπικής κλίμακας , ωστόσο υπάρχουν και κάποια προϊόντα που υποστηρίζουν το μοντέλο VPN τύπου client-to-LAN , δηλαδή στη μια άκρη του δικτύου βρίσκεται ο απομακρυσμένος χρήστης με κάποιο υπολογιστή client .



5. 4. ΤΑ ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ ΔΡΟΜΟΛΟΓΗΤΗ (Router –Based VPNs)

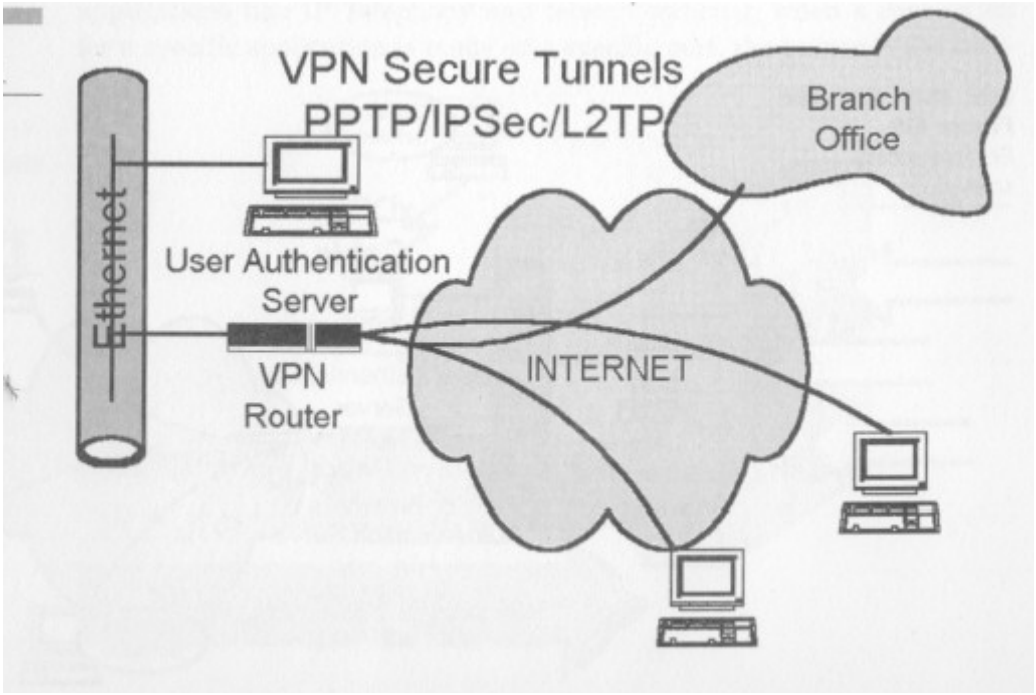
Σύμφωνα με την αρχιτεκτονική Εικονικού Ιδιωτικού Δικτύου που στηρίζεται στο δρομολογητή κάθε πακέτο πληροφορίας που μεταδίδεται εντός του δικτύου θα πρέπει να ελέγχεται από τον router ο οποίος αποτελεί τον απόλυτο διαχειριστή του κάθε πακέτου , υποστηρίζοντας ταυτόχρονα και το μηχανισμό κρυπτογράφησης του κάθε πακέτου .

Οι κατασκευαστές συνήθως παρέχουν δυο τρόπους υλοποίησης των εικονικών δικτύων που βασίζονται στο δρομολογητή . Κατά τον πρώτο τρόπο κατάλληλο λογισμικό ενσωματώνεται στον ήδη υπάρχοντα δρομολογητή του δικτύου αναλαμβάνοντας να διεκπεραιώσει τη λειτουργία της κρυπτογράφησης των μεταδιδόμενων πακέτων .

Σύμφωνα με τον δεύτερο τρόπο υλοποίησης της αρχιτεκτονικής router μια εξωτερική κάρτα με διάφορα κυκλώματα (circuits) ενσωματώνεται εντός της συσκευής του router . Η εξωτερική αυτή κάρτα περιλαμβάνει κεντρική μονάδα επεξεργασίας (CPU) που στοχεύει να αναλάβει την εκτέλεση της διεργασίας της κρυπτογράφησης με την οποία ήταν αρχικά επιφορτισμένη η μονάδα επεξεργασίας του router

Η ενσωμάτωση της εξωτερικής κάρτας πάνω στο router ενδείκνυται σε περιπτώσεις που το Εικονικό Δίκτυο έχει να αντιμετωπίσει πολλαπλές συνδέσεις από πολλούς απομακρυσμένους χρήστες οπότε απαιτείται αρκετά δυνατή επεξεργαστική ισχύς . Ωστόσο εάν μια επιχείρηση ήδη χρησιμοποιεί κάποιο router και θέλει να δημιουργήσει το εικονικό δίκτυο της θα πρέπει να σημειωθεί ότι συμφέρει να αγοράσει το κατάλληλο επιπρόσθετο λογισμικό καθώς διατηρεί κατά αυτόν τον τρόπο χαμηλό το κόστος αναβάθμισης .

Αλλά και στην τελευταία περίπτωση δεν μπορεί να διασφαλιστεί η ομαλή λειτουργία του εικονικού δικτύου όταν θα εμφανιστεί στο μέλλον κάποια επιπλοκή κατά τη λειτουργία του router , καθώς δε μπορεί από μόνο του το λογισμικό κρυπτογράφησης να αποτρέψει μια πιθανή κατάρρευση του Εικονικού Ιδιωτικού Δικτύου .



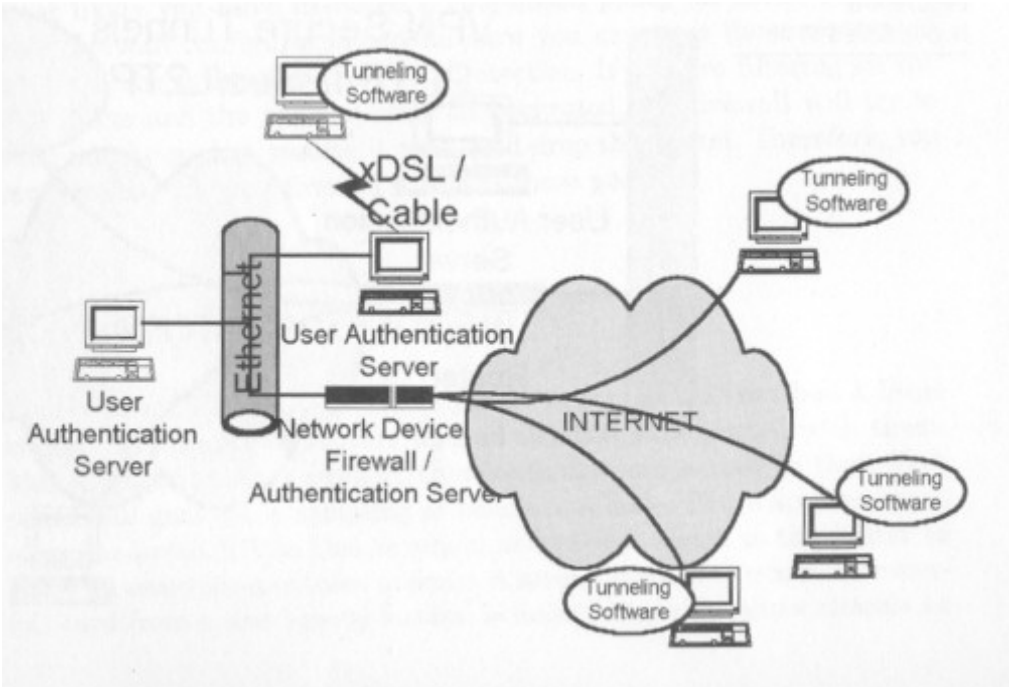
5. 5. ΤΑ ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ (Remote Access Based VPNs)

Τα εικονικά Ιδιωτικά Δίκτυα απομακρυσμένης πρόσβασης ονομάζονται αλλιώς και ιδιωτικά dial-up δίκτυα (VPDN) αφορούν κυρίως τους απομακρυσμένους χρήστες του δικτύου , συχνά αναφερόμενοι ως κινητοί χρήστες (mobile users) . Στο παρελθόν οι επιχειρήσεις υποστήριζαν την επικοινωνία του τοπικού τους δικτύου με τους απομακρυσμένους χρήστες διαμέσω των κοινών dial-up δικτύων όπως τα τηλεφωνικά δίκτυα με αποτέλεσμα ο χρήστης να πληρώνει κάποιο τέλος κλήσης κάθε φορά που συνδεόταν με το δίκτυο . Η τακτική αυτή ήταν αρκετά αντιοικονομική ιδιαίτερα κατά τις περίπτωση που απαιτούνταν διεθνείς κλήσεις .

Με την εμφάνιση όμως των Εικονικών Ιδιωτικών Δικτύων απομακρυσμένης πρόσβασης μπορεί πλέον ο απομακρυσμένος χρήστης να κάνει μια τοπική κλήση στον παροχέα υπηρεσιών του Διαδικτύου (ISP) αποκτώντας κατ` αυτόν τον τρόπο πρόσβαση στο δίκτυο κάποιας επιχείρησης . Έτσι μπορεί δηλαδή ο user να συνδεθεί με τον προσωπικό υπολογιστή του με κάποιο LAN διαμέσω του Διαδικτύου .

Τα VPN απομακρυσμένης πρόσβασης αποτελούν επέκταση των αρχικών δικτύων dial-up καθώς κατάλληλο λογισμικό πάνω στον προσωπικό υπολογιστή του κινητού χρήστη αναλαμβάνει να κάνει κλήση προς κάποιο ενδοεπιχειρησιακό δίκτυο διενεργώντας τη διαδικασία tunneling . Το tunnel όμως όπως φαίνεται και στην παρακάτω εικόνα μπορεί να προέρχεται και από μια σύνδεση διαφορετική από αυτή του Διαδικτύου , όπως για παράδειγμα από μια σύνδεση ISDN , από κάποια DSL ή από σύνδεση με κάποιο δίκτυο τύπου X . 25.

- \www.intel.com\5.htm----white paper on Vpn Architecture
- \newagent.com------On-Demand Multi-carrier MPLS IP-VPN Interconnect (overview)
- \ The VPN Consortium(VPNC) web site-----VPN Technologies

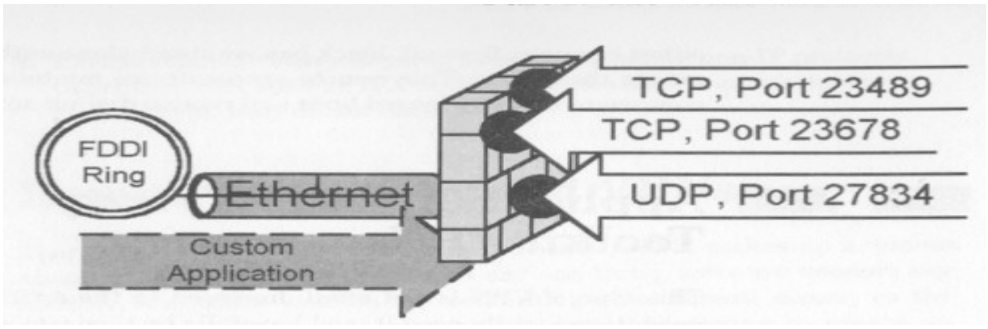


5. 6. Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ APPLICATION AWARE VPNs

Η αρχιτεκτονική των Application Aware ή αλλιώς Proxy Toolkit Εικονικών Δικτύων αναπτύχθηκε τα τελευταία χρόνια στα πλαίσια μιας προσπάθειας υποστήριξης από το VPN όλων εκείνων των νέων υπηρεσιών που απαιτούν αρκετά μεγάλο εύρος ζώνης μετάδοσης δεδομένων αλλά και δεν είναι συμβατές το ήδη υπάρχον μοντέλο πελάτη / εξυπηρετητή του Διαδικτύου .

Με βάση τη φιλοσοφία client / server του Internet , ο πελάτης (Client) μπορεί να ζητήσει από τον server την παροχή μιας συγκεκριμένης υπηρεσίας κάθε φορά οπότε εκείνος ανταποκρίνεται ανάλογα με την αίτηση του client . Ωστόσο με την εμφάνιση των καινούργιων πολυμεσικών υπηρεσιών , όπως το IP τηλέφωνο , οι ηλεκτρονικές συνδιαλέξεις κτλ , κάθε φορά που ο client ζητά την παροχή μιας τέτοιου είδους πολυμεσική υπηρεσία θα πρέπει το πρωτόκολλο διαχείρισης του δικτύου να εγκαθιστά πολλαπλές συνδέσεις που θα αφορούν μια και μόνο αίτηση παροχής υπηρεσίας.

Σύμφωνα με αρχιτεκτονική λειτουργίας των μέχρι στιγμής αναφερόμενων μοντέλων VPN ήταν αδύνατο να υποστηριχθούν τέτοιου είδους υπηρεσίες οπότε αναπτύχθηκε κάποια νέα φιλοσοφία λειτουργίας των VPNs σύμφωνα με την οποία δύναται πλέον να παρέχει ο server μια πολυμεσική υπηρεσία μέσα από την υποστήριξη νέων λειτουργιών από το πρωτόκολλο επικοινωνίας . Η αρχιτεκτονική αυτή ονομάστηκε Application Aware ενώ σε αρκετές παραλλαγές της χρησιμοποιήθηκε το ισχυρό πρωτόκολλο MPLS για την υποστήριξη υπηρεσιών ηλεκτρονικού εμπορίου , ηλεκτρονικής συνδιάσκεψης όπως και άλλων πολυμεσικών υπηρεσιών .



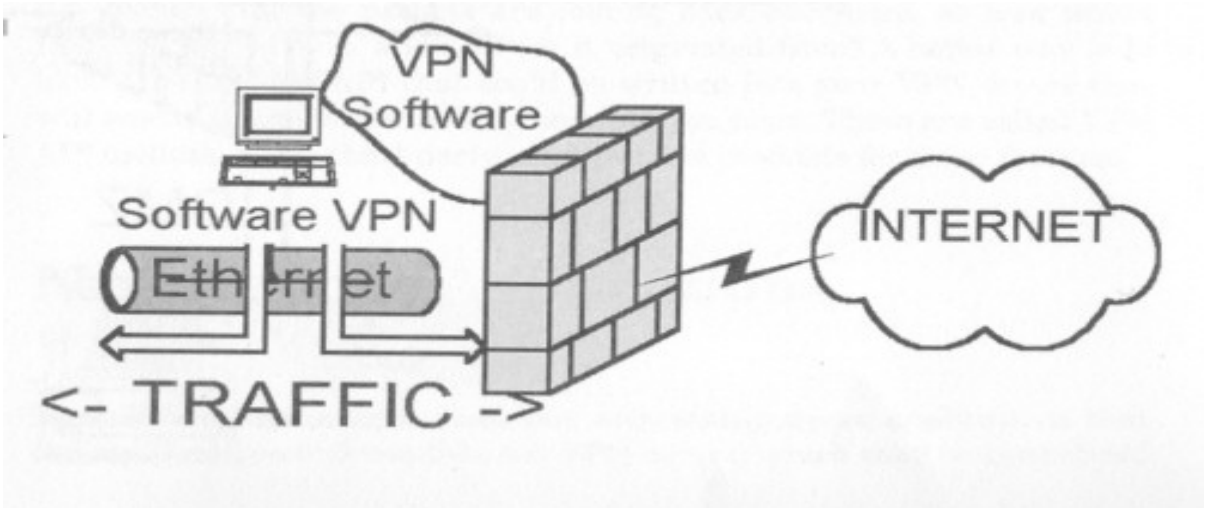
5. 7. ΤΑ ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ ΛΟΓΙΣΜΙΚΟ (Software Based VPNs)

Το Εικονικό Ιδιωτικό Δίκτυο αυτού του είδους ουσιαστικά υλοποιείται από κατάλληλο λογισμικό που δημιουργεί κάποιο tunnel με έναν υπολογιστή host από την άλλη μεριά της σύνδεσης, μεριμνώντας ταυτόχρονα για τη διαδικασία κρυπτογράφησης των πακέτων πληροφορίας. Δηλαδή η δημιουργία των tunnels συνεπάγεται την επικοινωνία του λογισμικού του client με το λογισμικό του server βάσει ενός κοινού πρωτοκόλλου (π .χ. του PPTP) .

Μόλις ξεκινήσει η μετάδοση της πληροφορίας από ένα host υπολογιστή εντός της επιχείρησης δημιουργείται αυτόματα μια σύνδεση με κάποιο server .Κατόπιν η πληροφορία κρυπτογραφείται και υφίσταται ενθυλάκωση ενώ στη συνέχεια δρομολογείται προς παραλήπτη . Αντίστροφα όταν κάποιος εξωτερικός client προσπαθήσει να επικοινωνήσει με τον εξυπηρετητή VPN της επιχείρησης αμέσως εξακριβώνεται οι αλγόριθμοι κρυπτογράφησης και πιστοποίησης της ταυτότητας του χρήστη και αμέσως πραγματοποιείται η επικοινωνία των δυο άκρων του VPN οπότε μπορεί πλέον να γίνει με ασφάλεια η μετάδοση της πληροφορίας .

Τα Software-based εικονικά δίκτυα παρέχουν τις λιγότερες υπηρεσίες σχετικά με τις υπόλοιπες αρχιτεκτονικές VPN ενώ ενδείκνυνται για μικρής ισχύος υπολογιστικά συστήματα που δεν έχουν τη δυνατότητα να υποστηρίξουν μεγάλη κυκλοφορία δεδομένων.

Τέλος όπως υπονοείται και από την περιγραφή του τρόπου λειτουργίας του software based εικονικού δικτύου η αρχιτεκτονική τους είναι κατάλληλη για συνδέσεις τύπου client-to-LAN .



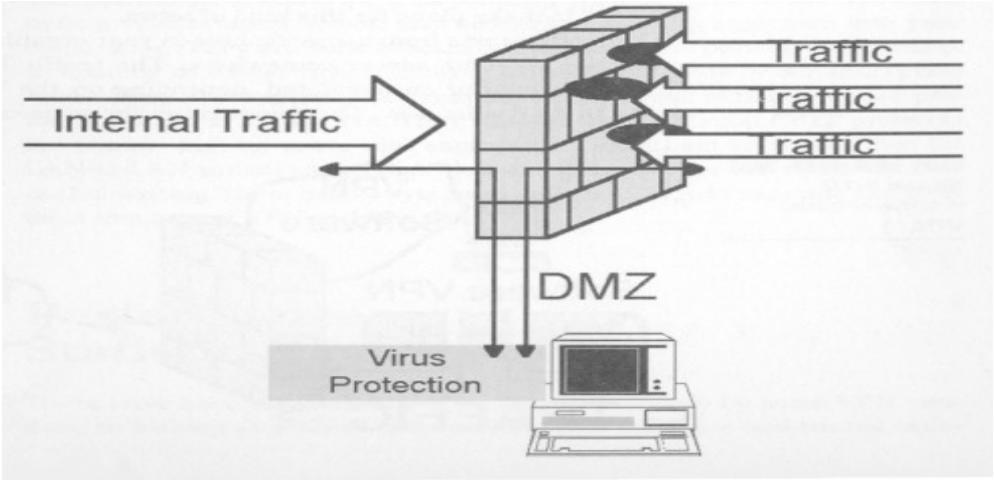
5 . 8. ΤΑ MULTISERVICE APPLICATION VPNs & ΤΑ TUNNEL SWITCHING VPNs

Οι δυο αρχιτεκτονικές εικονικών δικτύων που αναφέρονται στην ενότητα αυτή είναι παρόμοιες και ταυτόχρονα αρκετά διαδεδομένες τα τελευταία χρόνια όπου υπάρχει δυνατότητα υποστήριξης μεγάλης επεξεργαστικής ισχύος από του σύγχρονους υπολογιστές .

Συγκεκριμένα τα Multiservice Applications εικονικά δίκτυα επικεντρώνονται κυρίως στην προστασία του δικτύου από τους ολοένα και πιο επικίνδυνους ιούς . Η δυνατότητα επεξεργασίας και φιλτραρίσματος κάθε είδους πληροφορίας που προέρχεται από τον παγκόσμιο ιστό αποτελούν το πρώτιστο χαρακτηριστικό της αρχιτεκτονικής multiservice ενώ θα πρέπει να σημειωθεί ότι δεν

πρόκειται για μια εντελώς καινούργια αρχιτεκτονική αλλά για μια αναβαθμισμένη μορφή των ήδη υπαρχόντων firewall-based εικονικών δικτύων .

Όπως φαίνεται και από το διάγραμμα 5.7. α όλες οι πληροφορίες που εισέρχονται από το δημόσιο δίκτυο προς το ενδοεπιχειρησιακό δίκτυο αποκρυπτογραφούνται και αναλύονται πρώτα από το `` αντιβιοτικό`` πρόγραμμα που είναι ενσωματωμένο πάνω στο firewall του δικτύου . Κατόπιν μόλις επαληθευτεί η μη επικινδυνότητα της εισερχόμενης πληροφορίας αναφορικά για ιούς , μπορεί πλέον η πληροφορία να διαπεράσει το ενδοεπιχερησιακό δίκτυο



- \Cisco - Multiservice VPN Solution Overview.htm ---- multiservice VPN by Cisco
- \IEEE Computer Society -- An Approach to VPN (overview University of Napoli "Federico II")

\www.astaro.com ------ Astaro VPN (article)

- \A MOBILE PROVIDER VPN-- report DEPARTMENT OF TELEMATIC ENGINEERING OF THE TECHNICAL UNIVERCITY OF CATALONIA
- \www.adtran.com-----overview VPN (Adtran is a leading provider of network solutions)
- \ACERRA Course Offerings - VPN Technologies.htm ----- e-learning provider (ACERA)

Cisco - Cisco SMB Class VPN Solution Overview.htm

- \Cisco - VPN Solutions for Service Providers.htm
- \faq.htm ----What is VPN
- \Find VPN (Virtual Private Networks) An Introduction to Free.htm----ARTICLE (WEB HOSTING INDUSTRY NEWSMAGAZINE)
- \Find VPN (Virtual Private Networks) An Introduction to MPLS.htm

Αναφορικά με την αρχιτεκτονική **Tunnel Switching** θα πρέπει να αναφερθεί ότι πρόκειται για μια νεοεισερχόμενη αρχιτεκτονική εικονικού δικτύου στην αγορά η οποία συνεχώς επανασχεδιάζεται και αναβαθμίζεται με νέες λειτουργίες . Χωρίς να αναφερθούν εξειδικευμένες έννοιες που αφορούν τον τρόπο λειτουργίας της , θα πρέπει να σημειωθεί ότι πρόκειται για μια νέου είδους αρχιτεκτονική που προσπαθεί να συνδυάσει τα χαρακτηριστικά και της λειτουργίες όλων των προηγούμενων αρχιτεκτονικών όπως για παράδειγμα τύπου δρομολόγησης ή τύπου firewall πάνω σε μια μοναδική φυσική συσκευή δικτύου .

Το νέο αυτό μοντέλο VPN είναι κατασκευασμένο ώστε να μπορεί να εξυπηρετήσει χιλιάδες απομακρυσμένους χρήστες ενώ οι μηχανισμοί κρυπτογράφησης και ενθυλάκωσης θα είναι σχεδιασμένοι ώστε να μπορούν διαχειριστούν μια μεγάλη γκάμα πρωτοκόλλων δικτύου διαφορετικών από το IP πρωτόκολλο .

- \www.motorola.com---- MPLS Vpns White Paper
- \ An article on Secure VPN by the "International Journal Of Network Management"
- \www.atreus-systems.com---- Site-to-Site VPN (overview)
- \www.iec.org----- VPN overview (The International Engineering Concortium)
- \CHIP_OnLine.gr----Hardware Κρυπτογράφησης
- \www.eTone.gr----e-connectiom:Εικονικά Ιδιωτικά Δίκτυα (άρθρο)
- \www_symbolo_gr.htm----- περίληψη των VPN

6 . ΣΥΓΚΡΙΣΗ ΤΩΝ ΔΙΑΦΟΡΩΝ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ VPNs

Αρχιτεκτονική VPN	**Θετικά Χαρακτηριστικά**	**Αρνητικά Χαρακτηριστικά**
Hardware-Based VPN	• Μεγάλη αποδοτικότητα του VPN & υψηλή προστασία από ανεπιθύμητες συνδέσεις . • Αξιόπιστη κρυπτογράφηση των μεγάλου μεγέθους πακέτων πληροφορίας • Αξιόπιστη διαδικασία κρυπτογράφησης • Δυνατότητα αναβάθμισης	• Περιορισμένη ευελιξία σε ασυνήθιστες μορφές επιχειρησιακών δικτύων • Υψηλό κόστος εγκατάστασης • Μη υποστήριξη συνδέσεων τύπου ATM και FDDI • Πιθανή αναποτελεσμάτικότητα κατά τη μετάδοση μικρού μεγέθους πακέτων (64 bytes)
Software-Based VPN	• Μεγάλη γκάμα προγραμμάτων στην αγορά • Ευκολία εγκατάστασης • Υποστήριξη πολλών τύπων	• Καλή συμβατότητα μόνο με συσκευές & υπολογιστές του ιδίου κατασκευαστή • Μερικά λογισμικά δεν υποστηρίζουν διαχείριση

	επιχειρήσεων	απομακρυσμένης πρόσβασης
Router-Based VPN	• Δεν απαιτείται αγορά καινούργιων συσκευών hardware • Υψηλή προστασία από ανεπιθύμητες συνδέσεις • Χαμηλό κόστος εάν δεν αντικατασταθούν οι ήδη υπάρχοντες δρομολογητές	• Πιθανή αγορά πλακέτας κρυπτογράφησης • Πιθανή αναβάθμιση του ήδη υπάρχοντος router • Πιθανή έλλειψη απόδοσης
Αρχιτεκτονική VPN	**Θετικά Χαρακτηριστικά**	**Αρνητικά Χαρακτηριστικά**
Firewall-Based VPN	• Μεγάλη γκάμα firewalls ανάλογα με τα χαρακτηριστικά του αγοραστή-επιχείρησης • Δεν απαιτείται αντικατάσταση των ήδη υπαρχόντων συσκευών hardware	• Πιθανά προβλήματα προστασίας εξαιτίας ασυμβατότητας του λειτουργικού προγ/τος • Πιθανή αδυναμία διαχείρισης τους διαμέσω του δικτύου από απομακρυσμένο σταθμό εργασίας
Remote Access-Based VPN	• Ευκολία εγκατάστασης • Αρκετά χαμηλό κόστος εγκατάστασης	• Προβληματικότητα κατά τη συμπίεση κρυπτογραφημένων πακέτων πληροφορίας

7. Βιβλιογραφία & Ηλεκτρονικές Διευθύνσεις Που Χρησιμοποιήθηκαν

A) NETWORK DESIGN Principles & Applications
By Gilbert Held---------- BEST PRACTICE SERIES © 2000

B) THE ESSENTIAL GUIDE TO NETWORKING
By Jim Keogh----------PRENTICE HALL © 2001

Γ) ATM THEORY AND APPLICATIONS
By David McDysan and Darren Spohn----------McGRAW HILL SERIES © 1999

Δ) A GUIDE TO VIRTUAL PRIVATE NETWORKS
By Martin W.Murhammer , Tim A.Bourne , Tamas Gaidosch , Charles Kunzinger , Laura Rademacher , Andreas Weinfurter----------PRENTICE HALL © 1998

E) IMPLEMENTING VIRTUAL PRIVATE NETWORKS
By Steven Brown ----------McGRAW-HILL SERIES © 1999

----------E- Links----------

1. \Cisco - Multiservice VPN Solution Overview.htm ---- multiservice VPN by Cisco

2. \IEEE Computer Society ------ An Approach to VPN (overview University of Napoli "Federico II")

3. \www.astaro.com ------ Astaro VPN (article)

4. \A MOBILE PROVIDER VPN-- report DEPARTMENT OF TELEMATIC ENGINEERING OF THE TECHNICAL UNIVERCITY OF CATALONIA

5.\www.adtran.com-----overview VPN (Adtran is a leading provider of network solutions)

6.\ACERRA Course Offerings - VPN Technologies.htm ----- e-learning provider (ACERA)

7. \Cisco - Cisco SMB Class VPN Solution Overview.htm

8. \Cisco - VPN Solutions for Service Providers.htm

9. \faq.htm ----What is VPN

10. \Find VPN (Virtual Private Networks) An Introduction to Free.htm----ARTICLE (WEB HOSTING INDUSTRY NEWSMAGAZINE)

11. \Find VPN (Virtual Private Networks) An Introduction to MPLS.htm

12. \Find VPN (Virtual Private Networks) The Advantages of a VPN.htm

13. \Find VPN (Virtual Private Networks) What About VPN Security.htm

14. \Find VPN (Virtual Private Networks) What is VoIP __ Explain.htm

15. \HNS Review - MPLS and VPN Architectures, CCIP Edition.htm(SEARCH MACHINE)---REVIEW OF A BOOK"MPLS & VPN ARCHITECTURES" BY BERISLAV KUCAN

16. \IS Auditing Guideline Review of Virtual Private Networks.htm---A review on vpn by Information Systems Audit and Control Association

17. \Logtel Seminar New Technologies in IP Networking.htm--- e-seminar by Logtel computer communication group

18. \Pearson Books - MPLS and VPN Architectures.htm----review of book"MPLS and VPN Architectures
Ivan Pepelnjak, Jim Guichard

19. \TISC 2001 Seminars.htm---overview on vpn by The Internet Security Conference

20. \v2.htm--- white paper on IPSec

21. \v4.htm----IPSec Virtual Private Networks: Conformance and Performance Testing

22. \Virtual Private Networking.htm---review on VPN by WINDOWSECURITY.com

23. \www.infosyssec.net/infosyssec/secvpn1.htm---- article on Vpn by "theWHIR's" (findvpn)

24. \VPN Bibliographies - links and VPN article references.htm---- Te Security Portal for Information System Security Professionals

25. \VPN FAQ.htm----- BY ACTIUS SUPPORT vpn faqs

26. \ cisco.com--- A Comparison Between MPLs and IPSec (white paper)

28. \http://computer.org/internet ---- article " The Latest In Vpn" Part a & Part b

29. \ Remote Access Vpn Solutions (overview) By Check Point Software Technologies

30. \pdf file by Cisco " How Vpn Works"

31. \www.dataconnection.com----------"VPN Technologies-AComparison" (white paper)

32. \www.diversinet.com--- white paper-- "Passport Wireless VPN"

33. \www.intel.com\5.htm----white pper on Vpn Architecture

34. \newagent.com------On-Demand Multi-carrier MPLS IP-VPN Interconnect (overview)

35. \ The VPN Consortium(VPNC) web site-----VPN Technologies

37. \www.motorola.com---- MPLS Vpns White Paper

38. \ An article on Secure VPN by the "International Journal Of Network Management"

39. \www.atreus-systems.com---- Site-to-Site VPN (overview)

40. \www.iec.org----- VPN overview (The International Engineering Concortium)

41. \CHIP_OnLine.gr----Hardware Κρυπτογράφησης

42. \www.eTone.gr----e-connectiom:Εικονικά Ιδιωτικά Δίκτυα (άρθρο)

43. \www_symbolo_gr.htm----- περίληψη των VPN