Τ Ε Ι Π Α Τ Ρ Α Σ

Σχολη Διοικησης & Οικονομιας

Επιχειρηματικος Σχεδιασμος & Πληροφοριακων Συστηματων

Π Τ Υ Χ Ι Α Κ Η Ε Ρ Γ Α Σ Ι Α

«ΤΕΧΝΟΛΟΓΙΕΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ ΣΕ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΙΚΤΥΑ ΜΕ ΕΜΦΑΣΗ ΣΤΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ»

Παπανικολάου Χρήστος(Α.Μ:532)- Καραγιάννης Ευστράτιος(Α.Μ:677)

Επιβλέπων Καθηγητής:

ΓΑΜΒΡΙΛΗ ΜΑΡΙΑ

ΠΑΤΡΑ 2007

ΠΡΟΛΟΓΟΣ

Σκοπός της πτυχιακής εργασίας αυτής είναι η μελέτη του τρόπου λειτουργίας των VPN που χρησιμοποιούν οι επιχειρήσεις από πλευράς διαχείρισης, ασφάλειας και κινητικότητας. Υπάρχει αυτήν την περίοδο σημαντικό ενδιαφέρον για την επέκταση των εικονικών ιδιωτικών δικτύων όσο αφορά το θέμα της ασφάλειας. Στη σημερινή εποχή της διεθνούς διαδικτύωσης η ασφάλεια αποτελεί μείζον θέμα για κάθε επιχείρηση που σέβεται τον εαυτό της. Είναι πλέον καθημερινό φαινόμενο η εισβολή στα υπολογιστικά συστήματα ενός οργανισμού, και η καταστροφή και τροποποίηση δεδομένων. Επιπλέον, επιθέσεις με ιούς (viruses), hacking, cracking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service) έχουν πλέον γίνει συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπισή τους. Καθώς οι επιχειρήσεις βασίζονται όλο και περισσότερο στα πληροφοριακά τους συστήματα, οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων. Η διασύνδεση ιδιωτικών και δημόσιων δικτύων και ο διαμοιρασμός πόρων δυσκολεύει ακόμη περισσότερο τον έλεγχο της πρόσβασης σε ένα σύστημα. Οι τάσεις επέκτασης κατανεμημένων περιβαλλόντων έχουν αποδυναμώσει την αποτελεσματικότητα του κεντρικού ελέγχου και διαχείρισης των συστημάτων από πλευράς προστασίας τους . Όλα αυτά τα γεγονότα έχουν κάνει πολύ σημαντική την έννοια της ασφάλειας, και ουσιαστικά καθένας οφείλει να τη λάβει σοβαρά υπόψη.

Στο 1^{ο} κεφάλαιο αναφέρουμε τα είδη των δικτύων που μπορούν να υλοποιηθούν στις επιχειρήσεις καθώς και πως μπορούν να τις βοηθήσουν στην καλύτερη ανάπτυξή τους.

Στο 2^{ο} κεφάλαιο γίνεται λόγος για τα εικονικά ιδιωτικά δίκτυα (τον ορισμό των VPN, τους τύπους VPN)και συγκεκριμένα τον τρόπο που μπορούν να συνδεθούν οι επιχειρήσεις μεταξύ τους βάση αρχιτεκτονικών και διεθνών προδιαγραφών που υπάρχουν.

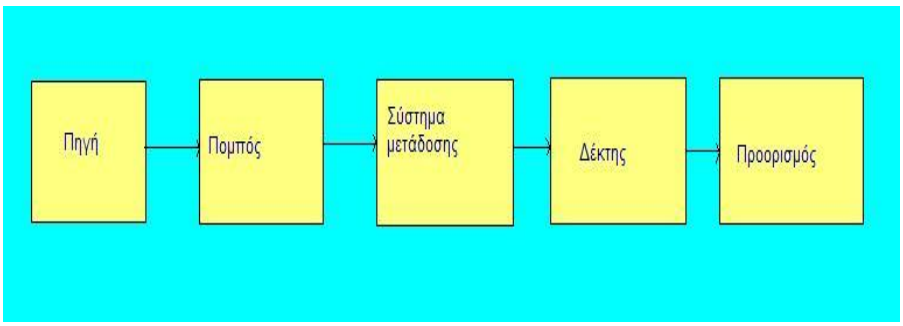
Στο 3^{ο} κεφάλαιο εισάγεται μια σημαντική παράμετρος για τα εικονικά ιδιωτικά δίκτυα η οποία είναι η ασφάλεια παράγοντας καταλυτικός ώστε να επιλέξει μια επιχείρηση την χρήση των δικτύων αυτών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ 1ο

1.ΔΙΚΤΥΑ

Τα δίκτυα είναι ένας συνδυασμός υλικού και λογισμικού που επιτρέπουν την επικοινωνία μεταξύ διαφορετικών υπολογιστικών συστημάτων. Ο βασικός σκοπός της επικοινωνίας είναι η ανταλλαγή δεδομένων μεταξύ δύο ή περισσότερων πλευρών. Στο επόμενο σχεδιάγραμμα φαίνεται ένα γενικό μοντέλο επικοινωνιών.



• **Πηγή**: Είναι η συσκευή που παράγει τα δεδομένα που θα μεταδοθούν. Παράδειγμα αποτελούν τα τηλέφωνα και οι προσωπικοί υπολογιστές.

• **Πομπός**: Συνήθως το σύστημα μετάδοσης δεν επιτρέπει τη μετάδοση δεδομένων στη μορφή που έχουν παραχθεί. Ο σκοπός του πομπού είναι να μεταλλάξει και να κωδικοποιήσει την πληροφορία με τέτοιο τρόπο ώστε να είναι δυνατό να μεταδοθεί από το χρησιμοποιούμενο σύστημα μετάδοσης. Για παράδειγμα ένα modem δέχεται μια ακολουθία δυαδικών συμβόλων και τη μετατρέπει σε ένα αναλογικό σήμα που μεταδίδεται στη συνέχεια μέσω του τηλεφωνικού δικτύου.

• **Σύστημα μετάδοσης**: Το σύστημα μετάδοσης μεταξύ του πομπού και του δέκτη είναι μεταβλητό και μπορεί να περιλαμβάνει από μόνο μία γραμμή μετάδοσης έως ένα πολύπλοκο δίκτυο που υλοποιεί τη σύνδεση.

• **Δέκτης**: Ο δέκτης δέχεται το σήμα από το σύστημα μετάδοσης και το μετατρέπει σε τέτοια μορφή ώστε να μπορεί να είναι κατανοητή από τη συσκευή προορισμού. Για παράδειγμα ένα modem λαμβάνει το αναλογικό σήμα που προέρχεται από το σύστημα μετάδοσης και το μετατρέπει σε μια σειρά από δυαδικά σύμβολα.

• **Προορισμός**: Παίρνει τα δεδομένα από το δέκτη.

Η παραπάνω περιγραφή κρύβει πολλές λεπτομέρειες υλοποίησης, τόσο του υλικού όσο και του λογισμικού που χρησιμοποιείται στα αναφερθέντα συστήματα.

1.1: Κατηγορίες Δικτύων

Η διάδοση των δικτύων κάνει επιτακτική την ανάγκη για ταξινόμηση τους όχι μόνο ανάλογα με τις εφαρμογές τους αλλά και με βάση τα τεχνικά τους χαρακτηριστικά. Εντούτοις, δύο χαρακτηριστικά των δικτύων που ξεχωρίζουν ως ιδιαιτέρως σημαντικά, είναι η τοπολογία και η κλίμακα.

1.1.1.: Τοπολογίες Δικτύων Υπολογιστών

Υπάρχουν γενικά δύο τύποι τοπολογιών στα δίκτυα υπολογιστών, τα Δίκτυα Εκπομπής και τα Δίκτυα Σημείου προς Σημείου.

Τα Δίκτυα Εκπομπής(broadcast networks) έχουν έναν μοναδικό δίαυλο επικοινωνίας που τον μοιράζονται όλες οι μηχανές του δικτύου. Ένας υπολογιστής ενός τέτοιου δικτύου αποστέλλει μηνύματα με την μορφή πακέτων στο δίκτυο και αυτά λαμβάνονται από όλους τους υπόλοιπους υπολογιστές του δικτύου. Με την παραλαβή του πακέτου κάθε υπολογιστής εξετάζει το πεδίο διεύθυνσης που αναγράφεται πάνω στο κάθε πακέτο και το οποίο είναι χαρακτηριστικό του τελικού προορισμού του. Αν το πακέτο προορίζεται για αυτόν τότε το

επεξεργάζεται, ενώ σε αντίθετη περίπτωση το αγνοεί.

Στα δίκτυα εκπομπής υπάρχει και η δυνατότητα της αποστολής ενός πακέτου σε όλα τα μέλη του δικτύου χρησιμοποιώντας κατάλληλο κωδικό στο πεδίο της διεύθυνσης του πακέτου, οπότε όλοι οι υπολογιστές του συγκεκριμένου δικτύου έχουν τη δυνατότητα να επεξεργαστούν την ίδια πληροφορία. Σε αυτήν τη περίπτωση μιλάμε για λειτουργία εκπομπής. Μερικά συστήματα εκπομπής υποστηρίζουν την μετάδοση σε ένα υποσύνολο υπολογιστών που ανήκουν σε ένα δίκτυο, οπότε μιλάμε για πολλαπλή διανομή, και αυτό γίνεται εφικτό αφιερώνοντας ένα bit διεύθυνσης ώστε να φανερώνει πολλαπλή διανομή.

Από την άλλη πλευρά, στα Δίκτυα Σημείου προς Σημείο(point to point networks) έχουμε πολλές συνδέσεις μεταξύ συγκεκριμένων ζευγών μηχανών. Κατά την διαδικασία μετάβασης ενός πακέτου από την πηγή στον προορισμό θα πρέπει να γίνεται σωστή επιλογή του υπολογιστή στον οποίο κατευθύνεται το πακέτο μιας και περνάει από διάφορους ενδιάμεσους υπολογιστές, καθώς και ορθή επιλογή της διαδρομής που θα ακολουθήσει το πακέτο μιας και συνήθως υπάρχουν πολλαπλές διαδρομές διαφορετικού μήκους μεταξύ των οποίων καλείται ο αλγόριθμος δρομολόγησης να επιλέξει.

Γενικά θα μπορούσαμε να πούμε ότι τα μικρότερα και γεωγραφικά περιορισμένα δίκτυα τείνουν να χρησιμοποιούν την εκπομπή, ενώ τα μεγαλύτερα δίκτυα είναι συνήθως σημείου προς σημείου.

1.1.2.: Κλίμακα Δικτύων Υπολογιστών

Όπως αναφέραμε και παραπάνω ένα ακόμη χαρακτηριστικό των δικτύων είναι η κλίμακά τους. Στην κορυφή της ιεραρχίας βάση αυτού του χαρακτηριστικού βρίσκονται οι μηχανές ροής δεδομένων, που είναι υπολογιστές υψηλού βαθμού παραλληλίας με πολλές λειτουργικές μονάδες να δουλεύουν για το ίδιο πρόγραμμα. Ακολουθούν οι πολλαπλοί υπολογιστές, που είναι συστήματα τα οποία επικοινωνούν στέλνοντας

μηνύματα μέσω μικρών και πολύ γρήγορων αρτηριών.

Πέρα από τους πολλαπλούς υπολογιστές είναι τα αληθινά δίκτυα στα οποία οι υπολογιστές επικοινωνούν ανταλλάσσοντας μηνύματα μέσω καλωδίων μεγαλύτερου μήκους.

Διαιρούνται σε τοπικά, μητροπολιτικά και ευρείας περιοχής, ενώ η σύνδεση δύο ή περισσοτέρων δικτύων ονομάζεται διαδίκτυο. Η απόσταση στην οποία εκτείνεται το καθένα από τα παραπάνω είναι σημαντική επειδή χρησιμοποιούνται διαφορετικές τεχνικές σε διαφορετικές κλίμακες και για τον λόγο αυτό παραθέτουμε τον παρακάτω πίνακα:

Απόσταση μεταξύ επεξεργαστών	**Θέση Επεξεργαστών**	**Παραδείγματα**
0,1 m	στην ίδια κάρτα	Μηχανή ροής δεδομένων
1 m	στο ίδιο σύστημα	Πολλαπλός υπολογιστής
10 m	στο ίδιο δωμάτιο	Τοπικό δίκτυο
100 m	στο ίδιο κτίριο	Τοπικό δίκτυο
1 km	στην ίδια περιοχή	Τοπικό δίκτυο
10 km	στην ίδια πόλη	Μητροπολιτικό δίκτυο
100 km	στην ίδια χώρα	Δίκτυο Ευρείας Περιοχής
1000 km	στην ίδια Ήπειρο	Δίκτυο Ευρείας Περιοχής
10000 km	στον ίδιο πλανήτη	Το Διαδίκτυο

Πίνακας 1:κλίμακες δικτύων

2.ΕΙΔΗ ΔΙΚΤΥΩΝ:

2.1 Δίκτυα προσωπικής περιοχής (Personal area networks)

Τα δίκτυα αυτά προορίζονται για ένα άτομο. Για παράδειγμα ένα ασύρματο δίκτυο που συνδέει έναν υπολογιστή με το ποντίκι, το πληκτρολόγιο και τον εκτυπωτή του είναι ένα δίκτυο προσωπικής περιοχής. Σε αυτή την κατηγορία ανήκει επίσης μια συσκευή PDA, που μπορεί να συνδέεται ασύρματα με το κινητό τηλέφωνο.

2.2 Τοπικά δίκτυα (local area networks)

Τα τοπικά δίκτυα (local area networks,LAN), είναι ιδιωτικά δίκτυα τα οποία βρίσκονται μέσα σε ένα μόνο κτίριο ή κτιριακό συγκρότημα, ή σε μια έκταση με μέγεθος μέχρι λίγα χιλιόμετρα. Χρησιμοποιούνται ευρέως για τη διασύνδεση προσωπικών υπολογιστών και σταθμών εργασίας σε γραφεία κι εργοστάσια εταιρειών, με στόχο την κοινοχρησία πόρων (για παράδειγμα, εκτυπωτών) και την ανταλλαγή πληροφοριών. Τα δίκτυα LAN διακρίνονται από τα άλλα είδη δικτύων με βάση τρία χαρακτηριστικά:

- Το μέγεθός τους
- Την τεχνολογία μετάδοσής τους
- Την τοπολογία τους

Τα δίκτυα LAN έχουν περιορισμένο μέγεθος, γεγονός που σημαίνει ότι ο χρόνος μετάδοσης στη χειρότερη περίπτωση βρίσκεται εντός συγκεκριμένων ορίων και είναι γνωστός εκ των προτέρων . Η γνώση αυτού του ορίου μας δίνει τη δυνατότητα χρήσης μερικών μεθόδων σχεδίασης που διαφορετικά δε θα ήταν εφικτές. Απλοποιεί επίσης και τη διαχείριση του δικτύου. Τα δίκτυα LAN μπορεί να χρησιμοποιούν μια τεχνολογία μετάδοσης η οποία συνίσταται σε ένα καλώδιο όπου είναι συνδεδεμένες όλες οι μηχανές. Τα παλαιότερα δίκτυα lan έχουν ταχύτητες από 10 Mbps έως 100 Mbps, έχουν χαμηλή καθυστέρηση (μικροδευτερόλεπτα ή

νανοδευτερόλεπτα), και παρουσιάζουν πολύ λίγα σφάλματα. Τα πιο πρόσφατα δίκτυα LAN λειτουργούν μέχρι και στα 10 Gbps.

Υπάρχουν διάφορες πιθανές τοπολογίες για τα δίκτυα LAN εκπομπής. Στις επόμενες εικόνες φαίνεται το δίκτυο διαύλου και το δίκτυο δακτυλίου. Σε ένα δίκτυο διαύλου, ανά πάσα στιγμή το πολύ μία μηχανή είναι ο κύριος (master) και επιτρέπεται να μεταδίδει δεδομένα. Όλες οι άλλες μηχανές πρέπει να αποφεύγουν τη μετάδοση την συγκεκριμένη χρονική στιγμή. Για να επιλύονται τυχόν συγκρούσεις όταν δύο ή περισσότερες μηχανές θέλουν να μεταδώσουν ταυτόχρονα, απαιτείται ένας μηχανισμός διαιτησίας. Ο μηχανισμός διαιτησίας μπορεί να είναι είτε συγκεντρωτικός είτε αποκεντρωμένος. Για παράδειγμα, το IEEE 802.3, που συνήθως ονομάζεται Ethernet, είναι ένα δίκτυο εκπομπής που βασίζεται σε δίαυλο με αποκεντρωμένο έλεγχο, και λειτουργεί συνήθως σε ταχύτητες από 10 Mbps έως 10 Gbps. Οι υπολογιστές σε ένα δίκτυο Ethernet μπορούν να μεταδίδουν όποτε θέλουν και αν δύο ή περισσότερα πακέτα συγκρουστούν, ο καθένας από τους υπολογιστές περιμένει απλώς για ένα τυχαίο χρονικό διάστημα και ξαναδοκιμάζει αργότερα.

α) Δίαυλος

β) Δακτύλιος

Ένας δεύτερος τύπος συστήματος εκπομπής είναι ο δακτύλιος (ring). Στα δίκτυα δακτυλίου το κάθε bit διαδίδεται μόνο του, χωρίς να περιμένει για το υπόλοιπο πακέτο στο οποίο ανήκει. Συνήθως το κάθε bit μπορεί να καλύψει ολόκληρο το δακτύλιο στο διάστημα που απαιτείται για τη μετάδοση λίγων μόνο bit, συχνά πριν καν μεταδοθεί ολόκληρο το πακέτο. Όπως και σε όλα τα συστήματα εκπομπής, απαιτούνται κάποιοι κανόνες διαιτησίας ώστε να αποφεύγονται οι ταυτόχρονες μεταδόσεις στο δακτύλιο.

Τα δίκτυα εκπομπής μπορούν να υποδιαιρεθούν περαιτέρω σε στατικά και δυναμικά, ανάλογα με το πώς γίνεται η εκχώρηση του καναλιού. Μια τυπική στατική εκχώρηση είναι να διαιρέσουμε το χρόνο σε διακριτά διαστήματα και αν χρησιμοποιήσουμε έναν αλγόριθμο εξυπηρέτησης εκ περιτροπής (round robin), επιτρέποντας σε κάθε μηχανή να εκπέμπει μόνο στο διάστημα που της αντιστοιχεί. Η στατική κατανομή σπαταλά τη χωρητικότητα του καναλιού στις περιπτώσεις που μια μηχανή δεν έχει τίποτα να πει όταν φτάνει η σειρά της, έτσι τα περισσότερα συστήματα προσπαθούν να εκχωρούν το κανάλι δυναμικά (δηλαδή κατόπιν αιτήσεως). Οι δυναμικές μέθοδοι εκχώρησης για ένα κοινό κανάλι είναι είτε συγκεντρωτικές είτε αποκεντρωμένες. Στη συγκεντρωτική μέθοδο εκχώρησης του καναλιού υπάρχει μια οντότητα – για παράδειγμα, μια μονάδα διαιτησίας του διαύλου – η οποία αποφασίζει ποιός έχει σειρά. Αυτό μπορεί να το επιτυγχάνει με το να δέχεται αιτήσεις και να παίρνει αποφάσεις σύμφωνα με κάποιον εσωτερικό αλγόριθμο. Στην αποκεντρωμένη μέθοδο εκχώρησης του καναλιού, δεν υπάρχει κάποια κεντρική οντότητα και η κάθε μηχανή πρέπει να αποφασίζει από μόνη της αν θα μεταδώσει.

2.3 Μητροπολιτικά δίκτυα (metropolitan area networks)

Ένα Μητροπολιτικό Δίκτυο (metropolitan area network ή MAN) είναι μια μεγαλύτερη εκδοχή ενός τοπικού δικτύου και συνήθως χρησιμοποιεί παρόμοια τεχνολογία. Μπορεί να καλύπτει ομάδα γειτονικών γραφείων μιας επιχείρησης ή μια πόλη και μπορεί να είναι είτε ιδιωτικό είτε δημόσιο. Ένα μητροπολιτικό δίκτυο μπορεί να υποστηρίζει δεδομένα καθώς και φωνή και ίσως ακόμη να σχετίζεται με την καλωδιακή τηλεόραση. Παράδειγμα δικτύου MAN είναι το δίκτυο καλωδιακής τηλεόρασης που υπάρχει σε πολλές πόλεις των Η.Π.Α.

2.4 Δίκτυα ευρείας περιοχής (wide area networks)

Το δίκτυο ευρείας περιοχής (wide area network), ή δίκτυο WAN, εκτείνεται σε μια μεγάλη γεωγραφική περιοχή, όπως μια χώρα ή μια ήπειρο. Στο δίκτυο WAN, οι μηχανές χωρίζονται στους υπολογιστές υπηρεσίας (hosts), που είναι οι μηχανές που εξυπηρετούν τους χρήστες του δικτύου (παράδειγμα, οι προσωπικοί υπολογιστές των χρηστών), και στο δίκτυο επικοινωνίας (communication subnet) ή για συντομία υποδίκτυο. Η δουλειά του υποδικτύου είναι να μεταφέρει μηνύματα ανάμεσα στους υπολογιστές υπηρεσίας. Ο διαχωρισμός των καθαρά επικοινωνιακών θεμάτων του δικτύου (το υποδίκτυο) από τα θέματα των εφαρμογών (τους υπολογιστές υπηρεσίας) απλοποιεί σημαντικά τη συνολική σχεδίαση του δικτύου.

Στα περισσότερα δίκτυα ευρείας περιοχής, το υποδίκτυο αποτελείται από δύο διακριτά συστατικά: Τις γραμμές μετάδοσης και τα στοιχεία μεταγωγής. Οι γραμμές μετάδοσης (transmission lines) μετακινούν bit ανάμεσα στις μηχανές. Μπορεί να υλοποιούνται με χάλκινα σύρματα, οπτικές ίνες ή ακόμα και με ασύρματες συνδέσεις. Τα στοιχεία μεταγωγής (switching elements) είναι εξειδικευμένοι υπολογιστές που συνδέουν τρεις ή περισσότερες γραμμές μετάδοσης. Όταν φτάνουν δεδομένα σε μια εισερχόμενη γραμμή, το στοιχείο μεταγωγής πρέπει να επιλέξει την εξερχόμενη γραμμή στην οποία θα τα προωθήσει. Το όνομα που χρησιμοποιείται σήμερα περισσότερο για τους υπολογιστές μεταγωγής είναι δρομολογητής (router).

Στα περισσότερα WAN το δίκτυο περιέχει πολλές γραμμές μετάδοσης, με κάθε γραμμή να συνδέει ένα ζεύγος δρομολογητών. Αν δυο δρομολογητές που δε μοιράζονται κάποια γραμμή μετάδοσης επιθυμούν να επικοινωνήσουν, θα πρέπει να το κάνουν έμμεσα, μέσω άλλων δρομολογητών. Όταν ένα πακέτο στέλνεται από ένα δρομολογητή σε κάποιον άλλο μέσω ενός η

περισσότερων ενδιάμεσων δρομολογητών, το πακέτο παραλαμβάνεται “αυτούσιο” σε κάθε ενδιάμεσο δρομολογητή, αποθηκεύεται εκεί μέχρι να απελευθερωθεί η απαιτούμενη γραμμή εξόδου, και μετά προωθείται. Τα υποδίκτυα που είναι οργανωμένα σύμφωνα με αυτή την αρχή ονομάζονται δίκτυα αποθήκευσης και προώθησης (store-and-forward) ή υποδίκτυα μεταγωγής πακέτων (packet-switched). Όλα σχεδόν τα δίκτυα ευρείας περιοχής χρησιμοποιούν υποδίκτυα αποθήκευσης και προώθησης. Όταν τα πακέτα είναι μικρά και έχουν όλα το ίδιο μέγεθος, συχνά ονομάζονται κελιά (cells).

Τα δίκτυα WAN δε χρησιμοποιούν όλα μεταγωγή πακέτων. Μια δεύτερη δυνατότητα για τα δίκτυα WAN είναι το δορυφορικό σύστημα. Κάθε δρομολογητής έχει μια κεραία μέσω της οποίας μπορεί να στέλνει και να λαμβάνει δεδομένα. Όλοι οι δρομολογητές μπορούν να ακούσουν την έξοδο από το δορυφόρο, ενώ σε μερικές περιπτώσεις μπορούν επίσης να ακούσουν τις μεταδόσεις των άλλων δρομολογητών προς το δορυφόρο. Μερικές φορές οι δρομολογητές είναι συνδεδεμένοι σε ένα μεγάλο υποδίκτυο από σημείο σε σημείο, με λίγους μόνο από αυτούς να διαθέτουν δορυφορική κεραία. Τα δορυφορικά δίκτυα είναι από τη φύση τους δίκτυα εκπομπής, και είναι ιδιαίτερα χρήσιμα όταν η ιδιότητα εκπομπής είναι σημαντική.

2.5 Διαδίκτυο (world wide web)

Ως διαδίκτυο (Internet) εννοείται κάθε συνένωση δύο ή περισσοτέρων δικτύων, όχι κατ’ ανάγκη ίδιας τεχνολογίας, έτσι ώστε να επιτυγχάνεται η επικοινωνία μεταξύ τους και να λειτουργούν σε λογικό επίπεδο σαν ένα δίκτυο. Για την επίτευξη της διαδικτύωσης των επιμέρους δικτύων χρησιμοποιούνται συσκευές τηλεπικοινωνιών όπως γέφυρες (bridges), πύλες(gateways), αναδιαμορφωτές(repeaters), δρομολογητές(routers), κλπ. Σήμερα με τον όρο διαδίκτυο εννοούμε το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων(net of nets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP, ενώ μπορεί να βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη.

Με το διαδίκτυο επιτυγχάνεται η διασύνδεση ετερογενών δικτύων Η/Υ (Internetworking Networks). Ο ιδιαίτερος χαρακτήρας του προκύπτει από την ανοχή που διαθέτει σε αναξιόπιστες συνδέσεις, καθώς σχεδιάστηκε έτσι ώστε να υποστηρίζει πολλαπλές εναλλακτικές συνδέσεις μεταξύ των υπολογιστών με αποτέλεσμα να διατηρεί τη λειτουργικότητά του ακόμα και με κατεστραμμένους κλάδους(π.χ. σε περίπτωση εκτεταμένων φυσικών καταστροφών ή πυρηνικών εκρήξεων).

Το πρωτόκολλο TCP/IP (Transmission Control Protocol / Internet Protocol), είναι αυτό που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και διαμεταγωγής δεδομένων στο Internet. Βασίζεται στη λογική του «πακέτου» : στο κόμβο του αποστολέα το μήνυμα μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του όπως (π.χ. η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Στο κόμβο του παραλήπτη τα πακέτα συναρμολογούνται για να σχηματιστεί το αρχικό μήνυμα. Φυσικά, η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο διαδίκτυο έχει τη δική του διεύθυνση επικοινωνίας (IP address). Με τον τρόπο αυτό, επιτεύχθηκε η δημιουργία κατανεμημένων δικτύων (distributed networks) τα οποία δεν εξαρτώνται από ένα κέντρο οργάνωσης /ελέγχου και άρα δεν χρειάζεται να στηρίζουν τη λειτουργία τους σε κάποιο κεντρικό υπολογιστή.

3. ΚΡΙΤΗΡΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ:

3.1 Σχήμα μετάδοσης:

- Σύγχρονη και ασύγχρονη μετάδοση:

Η μετάδοση μιας ροής από μια συσκευή σε μια άλλη μέσω μιας ζεύξης απαιτεί αρκετή συνεργασία και συνεννόηση μεταξύ των δυο πλευρών. Μία από τις πιο θεμελιώδεις απαιτήσεις είναι ο συγχρονισμός. Ο δέκτης πρέπει να γνωρίζει το ρυθμό στον οποίο παραλαμβάνονται τα bit, έτσι ώστε να μπορεί σε τακτά χρονικά διαστήματα να κάνει δειγματοληψία στην γραμμή, για να καθορίσει την τιμή του κάθε bit που λαμβάνεται. Δύο τεχνικές χρησιμοποιούνται ευρέως για αυτό το σκοπό.

Στην ασύγχρονη μετάδοση, κάθε χαρακτήρας δεδομένων αντιμετωπίζεται ανεξάρτητα. Κάθε χαρακτήρας αρχίζει με ένα bit έναρξης (start bit) που ειδοποιεί τον δέκτη ότι ένας χαρακτήρας καταφθάνει. Ο δέκτης κάνει δειγματοληψία σε κάθε bit του χαρακτήρα και έπειτα ψάχνει για την αρχή του επόμενου χαρακτήρα. Αυτή η τεχνική δε θα λειτουργήσει καλά για μακριές ενότητες (blocks) από δεδομένα επειδή το ρολόι του δέκτη μπορεί να χάσει το συγχρονισμό του με το ρολόι του πομπού. Ωστόσο, η αποστολή δεδομένων σε μεγάλες ενότητες (blocks) είναι αποδοτικότερη από την αποστολή δεδομένων κατά έναν χαρακτήρα τη φορά. Για μεγάλες ενότητες χρησιμοποιείται η σύγχρονη μετάδοση. Κάθε ενότητα δεδομένων είναι μορφοποιημένη ως ένα πλαίσιο που περιλαμβάνει μια σημαία (flag) έναρξης και μια λήξης. Κάποια μορφή συγχρονισμού, όπως η χρήση της κωδικοποίησης Manchester, χρησιμοποιείται.
Για να μεταδώσει μια συσκευή πάνω από ένα μέσο, πρέπει να συνδεθεί μέσω κάποιου είδους διεπαφής. Η διεπαφή καθορίζει όχι μόνο τα ηλεκτρικά χαρακτηριστικά του σήματος αλλά επίσης τα φυσικά μέσα σύνδεσης και τις διαδικασίες για την αποστολή και λήψη δεδομένων.

Η σύγχρονη μετάδοση πλεονεκτεί σε ρυθμό μεταφοράς πληροφορίας. Η απόδοση της σύγχρονης μετάδοσης είναι υψηλότερη αφού ο συγχρονισμός γίνεται μια φορά για κάθε τμήμα δεδομένων. Αντίθετα στην ασύγχρονη μετάδοση έχουμε πληροφορία συγχρονισμού για κάθε χαρακτήρα. Άλλο σημείο που υπερτερεί η σύγχρονη μετάδοση είναι σε μεθόδους διάγνωσης και διόρθωσης σφαλμάτων. Το μεγάλο πλεονέκτημα της ασύγχρονης μετάδοσης είναι η υλοποίησή της με μικρό

κόστος εξοπλισμού. Αυτός είναι ο λόγος για τον οποίο είναι ιδιαίτερα δημοφιλής σε μια μεγάλη κατηγορία υπολογιστικών συστημάτων και περιφερειακών συσκευών.

3.2 Τεχνολογία μετάδοσης δικτύων:

- Επικοινωνία με Σύνδεση ή Χωρίς Σύνδεση:

Σε ένα δίκτυο μεταγωγής με πακέτα, η επικοινωνία μπορεί να έχει δύο μορφές: με σύνδεση (connection oriented) ή χωρίς σύνδεση (connectionless).
Όταν η επικοινωνία γίνεται με σύνδεση, πριν αρχίσει η ανταλλαγή δεδομένων το δίκτυο ενημερώνεται και εγκαθίσταται ένα κανάλι επικοινωνίας. Στη συνέχεια η ροή των δεδομένων μπορεί να είναι συνεχής και το δίκτυο φροντίζει για τη σωστή αποστολή των πακέτων και πιθανώς και για την ελάχιστη ταχύτητα.
Αντίθετα, όταν η επικοινωνία γίνεται χωρίς σύνδεση, η ανταλλαγή των μηνυμάτων γίνεται χωρίς έλεγχο από το δίκτυο. Το δίκτυο απλώς αποστέλλει ανεξάρτητα πακέτα, χωρίς να ξέρει ότι ποια αποτελούν μέρος της ίδιας ροής δεδομένων προς έναν κόμβο. Αυτός ο τρόπος είναι ταχύτερος, όταν δεν πρόκειται να αποσταλούν πολλά δεδομένα, αλλά πάσχει από ασφάλεια.

4. ΑΞΙΟΠΟΙΗΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Αργά ή γρήγορα, οι περισσότερες επιχειρήσεις επενδύουν στην πληροφορική. Αυτό που καλείται να επιτύχει η πληροφορική είναι να ελαχιστοποιήσει το κόστος και τον κόπο, ενώ συγχρόνως να επιφέρει σημαντική πρόοδο ως προς την αποτελεσματικότητα της επιχείρησης.

4.1 Πλεονεκτήματα:

1. **Αυξάνει την ταχύτητα των δραστηριοτήτων της επιχείρησης.**

- Μπορεί να δημιουργήσει πρότυπα για όλα τα βασικά έγγραφα.

- Θα χρειάζεται μόνο να εισάγετε τις πληροφορίες (π.χ. τη διεύθυνση) μια φορά και έπειτα να τα χρησιμοποιείτε ξανά και ξανά.

2. **Βελτιώνει την ποιότητα της εργασίας.**

- Μπορεί να δημιουργήσει έγγραφα που εκφράζουν επαγγελματισμό.

3. **Διαχειρίζεται ηλεκτρονικά όλες τις πληροφορίες.**

- Τα έγγραφα μπορούν να κυκλοφορούν σε όλους στο γραφείο και να τροποποιούνται εύκολα.

Μπορείτε να παρακολουθείτε και να προγραμματίζετε την εργασία όλων των υπαλλήλων στην επιχείρηση, καθώς και να τηρείτε κάθε υπάλληλο.

4. **Διαμοιράζει πληροφορίες** :

- Η κύρια βάση δεδομένων, οι εκτυπωτές και ο αποθηκευτικός χώρος στο δίσκο – και το ημερολόγιο του γραφείου – μπορούν να χρησιμοποιούνται από όλους τους υπαλλήλους.

- Επίσης, οι πληροφορίες μπορούν να ενημερώνονται για να χρησιμοποιούνται από όλους τους υπαλλήλους της επιχείρησης.

5. **Επικοινωνία με το εξωτερικό περιβάλλον της επιχείρησης**.

- Δυνατότητα χρήσης του ηλεκτρονικού ταχυδρομείου για να επικοινωνούν άμεσα με άτομα σε ολόκληρο τον κόσμο με ελάχιστο κόστος.

- Εύρεση χρήσιμων πληροφοριών στο Διαδίκτυο.

- Βελτίωση της επαγγελματικής εικόνας μέσω παρουσιάσεων υψηλής ποιότητας ή ενός άριστου δικτυακού τόπου.

Στα πλαίσια του συνεχώς αυξανόμενου ανταγωνισμού στον τομέα των επιχειρήσεων, η χρήση των ηλεκτρονικών υπολογιστών έχει γίνει επιτακτική ανάγκη για την βιώσιμη ανάπτυξη και εξέλιξή τους. Πολλές εταιρείες διαθέτουν σημαντικό αριθμό υπολογιστών σε λειτουργία τόσο σε μικρή απόσταση όσο και σε μεγάλες αποστάσεις μεταξύ τους. Για παράδειγμα, μια εταιρεία με πολλά εργοστάσια μπορεί να έχει έναν υπολογιστή σε κάθε μέρος για να κρατά στοιχεία που έχουν να κάνουν με τα αποθέματα, να παρακολουθεί την παραγωγικότητα και να διεκπεραιώνει διάφορες εργασίες όπως η τοπική μισθοδοσία. Όπως γίνεται αντιληπτό από το παράδειγμα η χρήση δικτύων είναι επιτακτική και μία βιώσιμη λύση για την καλύτερη οργάνωση της επιχείρησης.

5. Επιχειρησιακά Δίκτυα (Business networks)

Στα πρώτα μοντέλα υπολογιστικών συστημάτων που χρησιμοποιήθηκαν από επιχειρήσεις ο καθένας από τους υπολογιστές αυτούς μπορούσε να αξιοποιείται ξεχωριστά από τους υπόλοιπους. Με την πάροδο όμως των χρόνων και την αλματώδη ανάπτυξη τόσο της πληροφορικής και των τηλεπικοινωνιών οι επιχειρήσεις και οι άλλοτε μικρομεσαίες εταιρείες, άρχισαν να αποκτούν άμεση πρόσβαση στην πληροφορία, να γιγαντώνονται και έτσι να προκύπτει το πρόβλημα του ορθού καταμερισμού των πόρων. Η διοίκηση τότε των επιχειρήσεων αυτών ήταν αυτή που αποφάσισε την διασύνδεση όλων των υπολογιστών με στόχο αφενός μεν να καταστούν

διαθέσιμα όλα τα προγράμματα, ο εξοπλισμός και προπάντων τα δεδομένα σε οποιονδήποτε στο δίκτυο ανεξαρτήτου φυσικής θέσεως του πόρου και του χρήστη, αφετέρου την απόκτηση της δυνατότητας εξαγωγής και συσχέτισης πληροφοριών που αφορούν ολόκληρη την επιχείρηση.

Ένα ακόμα πολύ θετικό στοιχείο για την λειτουργία μιας επιχείρησης που ανακύπτει από την χρήση των δικτύων υπολογιστών, είναι και η υψηλή αξιοπιστία που παρέχει ένα δίκτυο όσων αφορά την ασφάλεια διατήρησης των δεδομένων. Αυτό επιτυγχάνεται μέσω εναλλακτικών πηγών τροφοδοσίας και έχει σαν αποτέλεσμα ακόμη και στην περίπτωση που κάποια μονάδα επεξεργασίας βγει εκτός λειτουργίας, οι άλλες να είναι σε θέση να αναλάβουν την εργασία της.

Πολύ σημαντικός είναι και ο παράγοντας της εξοικονόμησης χρημάτων τόσο για τις επιχειρήσεις που ο κερδοσκοπικός τους χαρακτήρας επιβάλει κάτι τέτοιο όσο και για έναν οργανισμό με σημαντικό αριθμό εργαζομένων και κατ' επέκταση μεγάλο αριθμό υπολογιστικών μονάδων. Είναι γεγονός αδιαμφισβήτητο ότι οι μικροί υπολογιστές είναι πολύ καλύτεροι λόγω κόστους από τους μεγαλύτερους. Οι μεγάλοι υπολογιστές από την άλλη είναι σχεδόν δέκα φορές ταχύτεροι από τους προσωπικούς υπολογιστές αλλά κοστίζουν πολύ περισσότερο. Εξαιτίας αυτής της ανισορροπίας πολλοί σχεδιαστές συστημάτων κτίζουν συστήματα που απαρτίζονται από προσωπικούς υπολογιστές, έναν ανά χρήστη, με τα δεδομένα να κρατούνται σε έναν ή περισσότερους κοινόχρηστους εξυπηρετητές αρχείων. Δεν είναι άλλο από το πολύ γνωστό μοντέλο πελάτη-εξυπηρετητή όπου η επικοινωνία λαμβάνει χώρα με την ανταλλαγή μηνυμάτων αίτησης από τον πελάτη στον εξυπηρετητή. Ο εξυπηρετητής διεκπεραιώνει την εργασία και στέλνει πίσω την απάντηση.

Ένας επιπρόσθετος στόχος της δικτύωσης θα μπορούσαμε να πούμε ότι είναι και η ικανότητα βαθμιαίας αύξησης της επίδοσης του συστήματος, καθώς αυξάνει το φορτίο, με απλή πρόσθεση περισσοτέρων επεξεργαστών. Στην περίπτωση των μεγάλων υπολογιστών, όταν το σύστημα έχει εξαντλήσει τις

δυνάμεις του, πρέπει να αντικατασταθεί από ένα μεγαλύτερο, με μεγάλο κόστος και ακόμα μεγαλύτερη ενόχληση των χρηστών.

Τέλος, ένα ακόμα κέρδος που έχει μια επιχείρηση ή μια εταιρεία από την εγκατάσταση δικτύων υπολογιστών στους χώρους δραστηριοποίησής της, είναι ότι οι εργαζόμενοι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους άμεσα ακόμη και αν βρίσκονται σε μεγάλες αποστάσεις και να διεκπεραιώνουν εργασίες που απαιτούν ομαδική συμβολή και προσπάθεια για την επίτευξη των στόχων της επιχείρησης και που σε αντίθετη περίπτωση είναι χρονοβόρες και μη αποδοτικές.

Αναγκαία προϋπόθεση για τη μετάδοση ενός σήματος είναι η ύπαρξη του κατάλληλου μέσου μετάδοσης. Αντίστροφα, εάν δεν έχουμε κάποιο μέσο μετάδοσης, δεν είναι δυνατή η μετάδοση του σήματος .Τα δίκτυα στις επιχειρήσεις υλοποιούνται είτε ενσύρματα είτε ασύρματα. Είναι δύο εντελώς διαφορετικές επιλογές στο πώς μπορεί να σχεδιαστεί ένα δίκτυο σε μια επιχείρηση. Τα ενσύρματα δίκτυα περιλαμβάνουν ένα πλήθος υπολογιστικών διατάξεων και περιφερειακών συσκευών, οι οποίες συνδέονται μέσω γραμμών επικοινωνίας, έτσι ώστε να είναι δυνατή η ανταλλαγή πληροφοριών ανάμεσά τους. Τα ενσύρματα μέσα μετάδοσης που χρησιμοποιούνται στα δίκτυα επικοινωνιών είναι τα συνεστραμμένα ζεύγη καλωδίων (twisted pairs), τα ομοαξονικά καλώδια (coaxial cables) και οι οπτικές ίνες (fiber optics). Τα ασύρματα μέσα μετάδοσης που χρησιμοπιούνι δίκτυα επικοινωνιών είναι το IEEE 802.11a,το wi-fi ,το wi-max κ.α. Παρακάτω προσδιορίζονται τα πλεονεκτήματα και μειονεκτήματα των συνδέσεων αυτών.

6. ΕΠΙΛΟΓΗ ΑΣΥΡΜΑΤΟΥ - ΕΝΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

6.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΩΝ-ΕΝΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

1. Φορητότητα

Είναι το πλέον προφανές πλεονέκτημα ενός ασύρματου δικτύου. Επιτρέποντας στους χρήστες την πρόσβαση εν κινήσει, τα ασύρματα δίκτυα συμβάλλουν στη σημαντική αύξηση της παραγωγικότητας και στην δημιουργία προοπτικών για καινοτόμες χρήσεις. Φορητές εφαρμογές που απαιτούν πρόσβαση πραγματικού χρόνου σε κεντρικές βάσεις δεδομένων βρίσκουν ιδανικό περιβάλλον στην ασύρματη δικτύωση.

Τα ασύρματα συστήματα ενός τοπικού δικτύου (LAN) μπορούν να παρέχουν στους χρήστες του πρόσβαση σε οποιεσδήποτε πληροφορίες σε πραγματικό χρόνο για τη οργάνωση τους. Αυτή η κινητικότητα υποστηρίζει την παραγωγικότητα και τις δυνατότητες πολλών υπηρεσιών οι οποίες δεν είναι εφικτό να πραγματοποιηθούν με το καλωδιακό δίκτυο.

2. Γρήγορη και εύκολη εγκατάσταση

Η εγκατάσταση ενσύρματου δικτύου σε κτίριο (μετά την ολοκλήρωση της κατασκευής του τελευταίου) παρουσιάζει σημαντικές δυσκολίες, καθώς απαιτούνται το πέρασμα καλωδίων από τους τοίχους και άλλες μετατροπές από εξειδικευμένο προσωπικό. Τα ασύρματα δίκτυα προσφέρουν τη λύση, καθώς ο χρόνος εγκατάστασης είναι ελάχιστος ανεξάρτητα από την κτιριακή υποδομή. Η εγκατάσταση ενός ασύρματου συστήματος μπορεί να γίνει γρήγορα και εύκολα εξαλείφοντας την ανάγκη να περαστούν καλώδια μέσω των τοίχων και των ορόφων.

3. Ευελιξία

Η αναδιοργάνωση ενός ενσύρματου δικτύου είναι εξαιρετικά χρονοβόρα και δύσκολη, σε αντίθεση με εκείνη ενός ασύρματου δικτύου, όπου απλώς η μετακίνηση (ή προσθήκη) ενός δομικού στοιχείου αλλάζει και την έκταση του καλυπτόμενου χώρου. Η ασύρματη τεχνολογία επιτρέπει στο δίκτυο να πάει εκεί όπου το καλώδιο δεν μπορεί να φτάσει.

4. Κόστος

Σε πολλές περιπτώσεις, παρά τον ακριβό εξοπλισμό, η χρήση ασύρματου δικτύου ενδέχεται να μειώσει σημαντικά το κόστος δικτύωσης. Τα οφέλη, όμως, συνήθως είναι βραχυπρόθεσμα και προκύπτουν κυρίως από το μικρό κόστος επαναδιαμόρφωσης ενός υπάρχοντος δικτύου. Ειδική περίπτωση είναι η δημιουργία ασύρματης ζεύξης (wireless bridge) μεταξύ δύο ή περισσότερων εγκαταστάσεων μιας εταιρίας. Η χρήση ασύρματης ζεύξης κοστίζει όσο και το απαιτούμενο δομικό υλικό, ενώ η χρήση μίας μισθωμένης γραμμής (leased line) είναι εξαιρετικά δαπανηρή (σταθερό κόστος κάθε μήνα). Ακόμα, ενώ η αρχική επένδυση που απαιτείται για το δομικό υλικό του ασύρματου δικτύου μπορεί να είναι υψηλότερη από το κόστος των αντίστοιχων στοιχείων ενός καλωδιακού δικτύου, οι γενικές δαπάνες εγκατάστασης και οι δαπάνες συντήρησης είναι σημαντικά χαμηλότερες.

5. Αυξημένη αξιοπιστία (υπό προϋποθέσεις)

Σε πολλές περιπτώσεις ένα ασύρματο δίκτυο μπορεί να είναι πιο αξιόπιστο από ένα ενσύρματο και επιπλέον να διευκολύνει τον εντοπισμό προβλημάτων. Στα ενσύρματα δίκτυα η δυσλειτουργία υλικού (όπως σε καλώδια) είναι δύσκολο να εντοπιστεί, ενώ, εάν η δυσλειτουργία δεν είναι πλήρης, ενδεχομένως να οδηγήσει σε ακατανόητα προβλήματα. Βέβαια, τα ασύρματα δίκτυα έχουν να αντιμετωπίσουν και αυτά αντίστοιχα προβλήματα με κυριότερο τις παρεμβολές.

6. Αύξηση της παραγωγικότητας

Όλα τα παραπάνω πλεονεκτήματα έχουν ως σημαντικότερη συνέπεια την αύξηση της παραγωγικότητας. Καθώς οι δικτυακοί πόροι είναι πλέον προσβάσιμοι από παντού μέσα στο πεδίο εκπομπής, οι χρήστες αποδίδουν καλύτερα, διότι μπορούν να επιλέξουν οι ίδιοι που θα εργαστούν και θα συνεργαστούν. Αντί να σπαταλάτε χρόνος για την μετάβαση στη πηγή των δεδομένων (όπως σε κάποιο τερματικό), ο χρόνος αυτός αξιοποιείται για την επεξεργασία των δεδομένων αυτών.

7. Υλοποίηση πολλαπλών τοπολογιών

Τα ασύρματα συστήματα μπορούν να διαμορφωθούν με μια ποικιλία τοπολογιών ώστε να ικανοποιούν τις ανάγκες των εκάστοτε εφαρμογών και εγκαταστάσεων. Οι διαμορφώσεις των τοπολογιών είναι εύκολο να αλλαχθούν γιατί αποτελούνται από ανεξάρτητα ασύρματα δίκτυα τα οποία χρησιμοποιούνται τόσο από μικρές ομάδες χρηστών όσο και από χιλιάδες χρήστες σε πλήρη δίκτυα υποδομής επιτρέποντας την επικοινωνία μέσω του αέρα.

6.2 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΩΝ-ΕΝΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

1. Ασφάλεια

Αυτό είναι το πιο σημαντικό ζήτημα στις εφαρμογές δικτύωσης. Τα ασύρματα δίκτυα μειονεκτούν από πλευράς παρεχόμενης ασφάλειας, όχι όμως τόσο ώστε να μη χρησιμοποιούνται σε κρίσιμες εφαρμογές.

2. Ταχύτητα

Η μέγιστη ταχύτητα (με τα τωρινά πρότυπα) ενός ασύρματου δικτύου φτάνει τα 100 Mbps ενώ ένα

κλασσικό δίκτυο μπορεί και να φτάσει τα 10 Gbps (10 Gigabit Ethernet). Πάντως προς το παρόν το σχετικά μικρότερο εύρος ζώνης δεν αποτελεί περιοριστικό παράγοντα για την πλειονότητα των εφαρμογών.

3. Κόστος δομικών υλικών

Αν και μακροπρόθεσμα σε πολλές περιπτώσεις η εγκατάσταση ενός ασύρματου δικτύου κοστίζει λιγότερο από την εγκατάσταση ενός κλασσικού, το απαιτούμενο δομικό υλικό εξακολουθεί να είναι σημαντικά ακριβότερο.

4. Παρεμβολές

Σε γενικές γραμμές, τα ασύρματα δίκτυα είναι τουλάχιστον το ίδιο αξιόπιστα με τα ενσύρματα και πιο εύκολα στην αντιμετώπιση των προβλημάτων. Όμως είναι, ακόμα, ευάλωτα στις παρεμβολές. Οι παρεμβολές μπορεί να προέρχονται από άλλες ηλεκτρονικές και ηλεκτρομηχανικές συσκευές, ακόμα και από την γεωμετρία του χώρου λειτουργίας (για εσωτερικό δίκτυο) ή τις καιρικές συνθήκες (για εξωτερικό δίκτυο). Το κυριότερο πρόβλημα, ωστόσο, είναι η δυνατότητα που έχει ο οποιοσδήποτε, είτε κακόβουλα είτε ακούσια, με φτηνό και εύκολα διαθέσιμο εξοπλισμό να προκαλέσει προβλήματα ή και την πλήρη κατάρρευση του δικτύου, έστω και προσωρινά. Το νομικό καθεστώς δεν μπορεί να δώσει ολοκληρωμένη προστασία στον τομέα αυτό.

6.3 Τελική επιλογή ασύρματων-ενσύρματων

Με βάση την σύγκριση των παραπάνω, καταλήγουμε ότι μια επιχείρηση θα προτιμούσε να έχει κατά κύριο λόγο ασύρματη δικτύωση χωρίς να απορρίπτουμε σε κάποιες περιπτώσεις και την ενσύρματη δικτύωση. Ο κυριότερος παράγοντας είναι ότι καθημερινά χιλιάδες άνθρωποι χρειάζονται να βρίσκονται στο δίκτυο όλη την ώρα για να ανακτήσουν την πληροφορία που χρειάζονται μέσω των διαφόρων υπολογιστών τους (laptop, palmtop, notebook, shirt pocket, wristwatch), δίχως να είναι ενσύρματα συνδεδεμένοι στην επίγεια επικοινωνιακή

υποδομή. Συνεπώς γι' αυτούς του κινητούς χρήστες τα συννεστραμένα ζεύγη καλωδίων , τα ομοαξονικά καλώδια και οι οπτικές ίνες δεν αποτελούν καλή λύση. Γι' αυτούς λοιπόν η λύση είναι οι ασύρματες επικοινωνίες. Αν όμως λάβουμε υπόψη μας ότι σε ορισμένες περιπτώσεις η τοποθέτηση ινών είναι δύσκολη εξαιτίας κάποιων συνθηκών (μορφολογία εδάφους, βουνά, ζούγκλες, έλη κ.ο.κ.), τότε μπορούμε με βεβαιότητα να αποφανθούμε ότι οι ασύρματες επικοινωνίες είναι προτιμότερες.

Ο χώρος της ασύρματης επικοινωνίας και των προτύπων, τα οποία θα την καθορίζουν, εξελίσσεται συνεχώς. Οι μεγαλύτερες εταιρίες έχουν χωριστεί σε ομάδες και αναπτύσσουν ανταγωνιστικές τεχνολογίες με σκοπό την κυριαρχία σε μια αγορά που αναμένεται μέσα στα επόμενα χρόνια να εκτοξευτεί σε μερικά δισεκατομμύρια δολάρια. Σήμερα είναι διαθέσιμος ένας αριθμός από καινούργιες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και νέα πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές (notebook, laptop, palmtop) είναι διαθέσιμοι και ελκυστικοί, αφού έχουν πλέον συγκρίσιμο κόστος, υπολογιστική ισχύ και ποιότητα υπηρεσιών με τους σταθερούς υπολογιστές. Όλα αυτά έχουν σαν αποτέλεσμα την επιλογή για την υποστήριξη των ασύρματων επικοινωνιών.

7. ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Σε αυτό το κεφάλαιο αναφερθήκαμε στο πως υλοποιείται ένα δίκτυο καθώς και την μεγάλη σημασία που έχει στο ρόλο των επιχειρήσεων. Δηλαδή πως μπορεί να τις βοηθήσει ώστε να πετύχουν τους στόχους με ευκολότερο και γρηγορότερο τρόπο.
Στο επόμενο κεφάλαιο θα αναφερθούμε και σε ένα άλλο διαχωρισμό που μπορεί να γίνει μεταξύ δημόσιων και ιδιωτικών δικτύων και θα αναλύσουμε πως μπορούν οι επιχειρήσεις που βρίσκονται σε διαφορετικούς τόπους να συνδεθούν με ασφάλεια μέσω των vpn δικτύων και τις εφαρμογές αυτών.

ΜΕΡΟΣ 2ο

1. Εικονικά Ιδιωτικά Δίκτυα VPN

1.1 Εισαγωγή

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.

Ορισμός

Η παγκοσμιοποίηση της αγοράς και η εξέλιξη της τεχνολογίας ανάγκασε πολλές επιχειρήσεις να αλλάξουν τον τρόπο εργασίας τους. Οι περισσότερες επιχειρήσεις σήμερα έχουν ως κύριο μέλημα την γεωγραφική τους επέκταση και σε άλλες γεωγραφικές περιοχές πέρα από την έδρα τους. Οι επιχειρήσεις αυτές πρέπει πλέον να διατηρούν υποκαταστήματα σε πολλά σημεία της ίδιας χώρας ή ακόμα και του εξωτερικού, να έχουν εργαζόμενους που ταξιδεύουν, να μοιράζουν στοιχεία τους σε πελάτες και προμηθευτές.

Μέχρι και αρκετά πρόσφατα αυτό είχε ως επακόλουθο την χρήση μισθωμένων γραμμών (leased lines) με σκοπό την δημιουργία WAN (wide area network). Αυτές οι μισθωμένες γραμμές είχαν εύρος (bandwidth) από απλή ISDN (Integrated Services Digital Network, 128 Kbps) ως και OC3 (Optical Carrier-3, 155 Mbps) και παρείχαν

στις εταιρίες την δυνατότητα να μεγαλώσουν το ιδιωτικό δίκτυό τους πέρα από μία μέση μικρή γεωγραφική περιοχή. Ένα WAN έχει προφανή πλεονεκτήματα, εν συγκρίσει με ένα δημόσιο δίκτυο, όπως το Internet, όσον αφορά την αποτελεσματικότητα, την ασφάλεια, την εγκυρότητα και τις επιδόσεις. Αλλά η διατήρηση ενός WAN, ιδιαίτερα όταν χρησιμοποιούνται μισθωμένες γραμμές, αποτελεί μεγάλο έξοδο, το οποίο σταδιακά αυξάνεται όσο μεγαλώνει η απόσταση των γραφείων της επιχείρησης. 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.

Καθώς η δημοτικότητα του διαδικτύου μεγάλωνε οι εταιρίες αναζητούσαν να πετύχουν γρήγορο, ασφαλή και έγκυρη επικοινωνία μεταξύ των γραφείων τους σε οποιοδήποτε σημείο και αν βρίσκονται αυτά. Για να καλύψουν λοιπόν τις ανάγκες των εργαζομένων τους για επικοινωνία, αρκετές επιχειρήσεις άρχισαν να δημιουργούν τα δικά τους εικονικά ιδιωτικά δίκτυα, τα Virtual Private Networks ,VPN για να προσαρμοστούν στις ανάγκες των απομακρυσμένων υπαλλήλων και γραφείων.

Θα μπορούσαμε να ορίσουμε ένα Virtual Private Network ως εξής:

Ένα **Virtual Private Network (VPN)** είναι ένα προσωπικό δίκτυο, το οποίο χρησιμοποιεί ένα πιο ευρύ (δημόσιο) δίκτυο, όπως είναι το Internet, προκειμένου να επικοινωνεί με άλλα sites ή απομακρυσμένα δίκτυα. Αντί της χρήσης μίας μοναδικά αφιερωμένης γι' αυτό τον σκοπό, πραγματικής σύνδεσης, όπως η μισθωμένη γραμμή (leased line), το VPN χρησιμοποιεί εικονικές συνδέσεις δρομολογημένες μέσω του διαδικτύου, από το ιδιωτικό δίκτυο της εταιρίας προς την απομακρυσμένη σελίδα ή εργαζόμενο.

Όπως παρατηρούμε η φράση Virtual Private Network απαρτίζεται από τους όρους virtual, private, network. Η σημασιολογία τους φαίνεται παρακάτω.

Virtual: Ο όρος virtual σημαίνει εικονικό δηλαδή κάτι μη πραγματικό. Έχει δοθεί αυτός ο όρος επειδή 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 LANs. Το δίκτυο υφίσταται, μεταβάλλεται, τροποποιείται ανάλογα με το σημείο και το χρόνο που γίνεται η σύνδεση χρησιμοποιώντας εξωτερικό εξοπλισμό (του ISP) και όχι κατά ανάγκη της ίδιας της εταιρίας.

Private: 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.

Network: Ένα δίκτυο αποτελείται από δύο ή περισσότερες συσκευές που μπορούν ελεύθερα και ηλεκτρονικά να επικοινωνήσουν η μια με την άλλη μέσω των καλωδίων ή ασύρματα. Ένα VPN είναι ένα δίκτυο. Μπορεί να διαβιβάσει πληροφορίες πέρα από μεγάλες αποστάσεις αποτελεσματικά και αποδοτικά.

1.2 Ιστορία των VPN

Ο όρος VPN άρχισε να εμφανίζεται στις αρχές του 1997, αλλά υπάρχουν σημαντικές διαφωνίες σχετικά με την παραπάνω πρόταση. Αυτό οφείλεται στο ότι τα VPN στηρίζονται κυρίως στη σουίτα πρωτοκόλλων του TCP/IP, αν και υπάρχουν και υλοποιήσεις που αφορούν και άλλες τεχνολογίες, όπως ATM ή Frame Relay. Επίσης η βασική έννοια της κρυπτογράφησης και πολλές τεχνικές που χρησιμοποιούνται για την υλοποίησή της έχουν εξελιχθεί πολύ πριν την εμφάνιση του TCP/IP. Ιστορικά ένας πρόγονος των VPN είναι το Public Data Network (PDN) και συγκεκριμένα το Internet. Το Internet αποτελεί ένα παράδειγμα ευρείας διασύνδεσης καθώς το δίκτυο επιτρέπει σε κάθε οντότητά του να

ανταλλάξει δεδομένα με οποιαδήποτε άλλη οντότητα. Η παραλληλία του με το υπάρχον τηλεφωνικό δίκτυο είναι εμφανής. Το PDN δεν έχει έμφυτες ικανότητες διαχωρισμού της κυκλοφορίας μέσα σε αυτό και οποιαδήποτε αλλαγή στο καθεστώς επίτρεψης οποιασδήποτε σύνδεσης είναι αποκλειστική ευθύνη των οντοτήτων. Το περιβάλλον του PDN βασίζεται πάνω σε ένα κοινό τρόπο διευθυνσιοδότησης και σε μια κοινή ιεραρχία δρομολόγησης που επιτρέπει στα switching elements να καθορίσουν τη θέση των διασυνδεδεμένων οντοτήτων. Όλες οι οντότητες του δικτύου έχουν πρόσβαση σε κοινή υποδομή που αποτελείται από στοιχεία δρομολόγησης και κυκλώματα.

1.3 Προβλήματα και λόγοι δημιουργίας VPN

Το πρόβλημα του παραπάνω δικτύου PDN είναι ότι η ευρεία πρόσβαση που προσφέρει δημιουργεί περιορισμούς στο ποιες ανάγκες των χρηστών μπορούν να καλυφθούν. Η κυριότερη ανάγκη που δεν μπορεί να καλυφθεί είναι αυτή της κρυπτογράφησης των δεδομένων. Συγκεκριμένα το Internet δεν είναι η καλύτερη λύση για οργανισμούς που θέλουν να χρησιμοποιήσουν ένα δίκτυο για ένα κλειστό σύνολο χρηστών και για εφαρμογές ιδιωτικού χαρακτήρα, όπως η διασύνδεση γεωγραφικά απομακρυσμένων γραφείων μιας εταιρείας. Τότε τα προβλήματα που εμφανίζονται είναι το φτωχό Quality of Service, η χαμηλή διαθεσιμότητα και η αξιοπιστία του δικτύου, η χρήση τρόπων διευθυνσιοδότησης και πρωτοκόλλων που είναι γνωστά σε όλους τους χρήστες, η μη κρυπτογράφηση δεδομένων που κυκλοφορούν μέσα στο δίκτυο και η δυνατότητα καταγραφής τους από τρίτους. Επίσης μια εφαρμογή κάποιου χρήστη μπορεί να έχει διαφορετικές απαιτήσεις διαχείρισης του δικτύου ή απόδοσης από αυτές που προσφέρονται από το PDN. Η εκπλήρωση αυτών των αναγκών οδηγούσε στη χρήση ιδιωτικών δικτύων υλοποιημένων με μισθωμένες γραμμές, αλλά αυτή η λύση επιβάρυνε την εταιρεία με το κόστος της μίσθωσης γραμμών και της διαχείρισης του δικτύου από ειδικευμένο προσωπικό. Η αύξηση των απομακρυσμένων χρηστών απαιτούσε επέκταση της υπάρχουσας υποδομής και καθώς οι τοποθεσίες τους ήταν γεωγραφικά

διεσπαρμένες αυτό προκαλούσε δυσανάλογη αύξηση του κόστους χρήσης του δικτύου. Σε τέτοιες περιπτώσεις η διαχείριση του δικτύου γίνεται πολύ δύσκολη.

Η χρήση της υπάρχουσας υποδομής άρχισε να διαφαίνεται σαν η μοναδική λύση μείωσης του κόστους και των προβλημάτων επέκτασης. Η χρήση της έφερε στην επιφάνεια τα εγγενή προβλήματα αξιοπιστίας, και έλλειψης κρυπτογράφησης δεδομένων με αποτέλεσμα να απαιτείται η ανάπτυξη νέων τεχνολογιών. Η νέα τεχνολογία που αντιπροσωπεύεται από τα VPN προσπαθεί να εφαρμόσει τεχνικές κρυπτογραφίας, κατηγοριοποίησης των πληροφοριών και κατανομής υπηρεσιών σε κατηγορίες χρηστών με τέτοιο τρόπο ώστε να αντιμετωπίζει ως ένα βαθμό τα προβλήματα του υποστρώματος το οποίο τελικά αναλαμβάνει την μεταφορά της πληροφορίας. Βέβαια τα VPN δεν αποτελούν πανάκεια καθώς υπάρχουν εφαρμογές με απαιτήσεις που δεν μπορούν να καλυφθούν. Μοναδική λύση τότε αποτελούν τα ιδιωτικά δίκτυα.

2. VPN (Εικονικά ιδιωτικά δίκτυα)

2.1 Απαιτήσεις από ένα VPN

Τα VPN αποτελούνται από υλικό και λογισμικό το οποίο καλείται να ικανοποιήσει ένα σύνολο απαιτήσεων που θα κάνουν το VPN εύκολο στη χρήση και στη συντήρηση, ασφαλές και διαθέσιμο στους χρήστες. Μέσα από μια μελέτη των αναγκών του οργανισμού θα προκύψει ένα σύνολο χαρακτηριστικών για το VPN που θα εγκαταστήσει. Ο οργανισμός μπορεί είτε να υλοποιήσει το VPN με δικά του μέσα είτε να αναθέσει την εργασία σε έναν παροχέα VPN υπηρεσιών, που μπορεί να είναι ένας παροχέας Internet υπηρεσιών (ISP).

Στην τελευταία περίπτωση υπάρχουν ειδικές συμφωνίες (Service Level Agreements - SLAs) μεταξύ του χρήστη και του ISP, που περιέχουν τις απαιτήσεις του πρώτου και τις αντίστοιχες δεσμεύσεις του δεύτερου. Τα SLA είναι το μοναδικό μέσο στη διάθεση του χρήστη με το οποίο θα εξασφαλίσει την παροχή των υπηρεσιών από τον παροχέα. Επιβάλλεται ο χρήστης να βρει

τρόπους μέτρησης και παρακολούθησης αν όντως ο παροχέας εκπληρώνει τις υποχρεώσεις του. Αν η υλοποίηση του VPN αφορά πολλούς ISP τότε θα πρέπει ο χρήστης στη σύνταξη του SLA να προνοήσει για την εξασφάλιση της διασύνδεσής τους και της απόδοσης του τελικού συστήματος. Από την άλλη μεριά ο παροχέας βρίσκεται αντιμέτωπος με την πρόκληση της τήρησης των διαφόρων SLA που έχει αναλάβει. Το μεγάλο πρόβλημα που αποτελεί τροχοπέδη στην τήρηση κάποιων απαιτήσεων των SLA είναι το χαρακτηριστικό του best effort του Internet. Έτσι ο παροχέας πρέπει να αναπτύξει τεχνικές διαφοροποίησης των υπηρεσιών που προσφέρει ή να κατασκευάσει το δίκτυό του με τέτοιο τρόπο ώστε να εξασφαλίσει ένα καλό λόγο των απαιτήσεων των χρηστών του προς τις δυνατότητες διαχείρισης του φορτίου που περνά από αυτόν.

Η υλοποίηση ενός VPN πρέπει να υποστηρίζει τα παρακάτω χαρακτηριστικά:

2.1.1. Διαθεσιμότητα (Availability)

Το VPN πρέπει να προσφέρει πρόσβαση καθ' όλη τη διάρκεια του 24ώρου. Αυτό συνεπάγεται ότι θα πρέπει να ικανοποιεί κάθε αίτηση για σύνδεση, οποτεδήποτε αυτή εμφανιστεί. Η διαθεσιμότητα δεν εξαρτάται μόνο από την ικανότητα του παροχέα να κρατά το δίκτυό του σε συνεχή λειτουργία, καθώς κάποια προβλήματα οφείλονται σε παράγοντες εκτός ελέγχου του. Η περίπτωση χρήσης του Internet ως υποδομή είναι ένα τέτοιο παράδειγμα.

2.1.2. Έλεγχος (Control)

Ένα VPN μπορεί είτε να βρίσκεται κάτω από τον έλεγχο του παροχέα, είτε κάτω από τον έλεγχο του τομέα υποστήριξης δικτύου της εταιρείας. Συνήθως υπάρχει η αντίληψη από τα διοικητικά στελέχη ότι η διαχείριση του VPN από προσωπικό εκτός εταιρείας δημιουργεί περισσότερους κινδύνους επιθέσεων. Στην πραγματικότητα η επιλογή της διαχείρισης από τρίτους και συγκεκριμένα από τον φορέα υλοποίησης του VPN

έχει πολλά πλεονεκτήματα. Η μεγάλη εμπειρία και εξειδίκευση των τεχνικών εξασφαλίζει γρήγορη υλοποίηση και καλή λειτουργία του VPN. Οι εφαρμογές επόπτευσης της κυκλοφορίας και συναγερμού μπορούν να εξασφαλίσουν ένα καλό επίπεδο ασφάλειας. Η δεύτερη περίπτωση έχει το πλεονέκτημα του πλήρη ελέγχου του VPN αλλά θα πρέπει να ληφθούν σοβαρά υπόψη ο χρόνος εκπαίδευσης του προσωπικού, το κόστος απόκτησης του εξοπλισμού και ο χρόνος μέχρι να κριθεί επιχειρησιακό το δίκτυο.

Συμβατότητα (Compatibility)

Το VPN πρέπει να είναι συμβατό με το ήδη υπάρχον δίκτυο του χρήστη. Όταν υπάρχει χρήση διαφορετικών πρωτοκόλλων θα πρέπει να γίνουν οι απαραίτητες ενέργειες ώστε να διασυνδεθούν τα δύο δίκτυα. Για παράδειγμα μπορεί το VPN να στηρίζεται στο IP, ενώ το δίκτυο του χρήστη στο IPX. Η χρήση ενός gateway λύνει το πρόβλημα συμβατότητας προσθέτοντας ένα ακόμη επίπεδο στο σχεδιασμό και την υλοποίηση. Επίσης το δίκτυο πρέπει να φτάνει μέχρι το επίπεδο δικτύου (network layer) του προτύπου OSI του οργανισμού ISO.

2.1.3. Ασφάλεια (Security)

Ένα VPN δεν αποτελεί ιδιωτικό δίκτυο του χρήστη όπως ήδη έχει αναφερθεί. Η χρήση της κοινής υποδομής για τη μεταφορά πληροφοριών καθιστά δυνατή την υποκλοπή τους από τρίτους. Η ασφάλεια αναφέρεται σε όλες τις ενέργειες που εκτελούνται από τα στοιχεία του VPN, όπως για παράδειγμα είναι η διαδικασία κρυπτογράφησης των δεδομένων ή η διαδικασία πιστοποίησης των χρηστών του δικτύου. Βέβαια οι απαιτήσεις για ασφάλεια μπορεί να μην ικανοποιούνται αν η πλατφόρμα που θα εγκατασταθεί το VPN παρουσιάζει αδυναμίες. Αν ένα VPN υλοποιηθεί πάνω σε κάποιο λειτουργικό σύστημα τότε πρέπει να αντιμετωπιστούν τα πιθανά του προβλήματα ασφαλείας, διαφορετικά η χρήση του VPN θα είναι ανώφελη. Είναι φανερό ότι οι απαιτήσεις ασφάλειας δεν αφορούν μόνο την πολιτική του VPN στο θέμα αυτό αλλά και τα μέσα του χρήστη τα οποία θα υποστηρίξουν το δίκτυο.

2.1.4. Διαλειτουργικότητα (Interoperability)

Καθώς τα VPN είναι μια νέα τεχνολογία από πλευράς υλοποίησης προκύπτουν πολλά θέματα συμβατότητας από τη χρήση διαφόρων προτύπων κρυπτογράφησης και ασφαλείας. Υπάρχουν πολλά προϊόντα στην αγορά με αποτέλεσμα να είναι δύσκολη η επιλογή κάποιου από αυτά. Η έλλειψη πιστοποίησης σε κάποια από αυτά δεν εξασφαλίζει το ότι καλύπτουν τα πρότυπα ασφαλείας. Υπάρχουν βέβαια οργανισμοί πιστοποίησης που αναλαμβάνουν τον έλεγχο των προϊόντων και εκδίδουν πιστοποιητικά που δείχνουν τη συμφωνία του προϊόντος με τα διάφορα πρότυπα.

2.1.5. Αξιοπιστία (Reliability)

Ένα VPN πρέπει να προσφέρει εγγυήσεις για αξιόπιστη λειτουργία ειδικά όταν υλοποιείται από κάποιον ISP, καθώς τότε η λειτουργία του εξαρτάται σε ένα σημαντικό βαθμό από αυτόν. Αν το δίκτυο σταματήσει να λειτουργεί τότε ο χρήστης το μόνο που μπορεί να κάνει είναι να περιμένει από τον ISP να λύσει το πρόβλημα. Ο χρόνος εξυπηρέτησης εξαρτάται από τον αριθμό των χρηστών που υποστηρίζει ο ISP και από το πόσο εύκολα μπορεί να διαθέσει πόρους για τη λυση του προβλήματος.

2.1.6. Πιστοποίηση δεδομένων και χρηστών (Data and User authentication)

Είναι πολύ σημαντικό σε κάθε υλοποίηση VPN να προσφέρονται και οι δύο υπηρεσίες, επειδή αποτελούν σημαντικές πτυχές της ασφάλειας που θα προσφέρεται. Η πιστοποίηση δεδομένων αφορά την επιβεβαίωση ότι τα δεδομένα έχουν ληφθεί στο σύνολό τους και ότι δεν έχουν μεταβληθεί κατά τη μεταφορά τους. Πιστοποίηση χρήστη είναι η διαδικασία χορήγησης άδειας πρόσβασης στο δίκτυο. Αν ο χρήστης βρίσκεται εκτός του εταιρικού δικτύου τότε πρέπει να γίνεται ασφαλής και αξιόπιστη εξακρίβωση της ταυτότητάς του πριν του παραχωρηθεί το δικαίωμα της πρόσβασης. Επίσης πρέπει να εξακριβωθούν και τα δικαιώματα που έχει από τη στιγμή

που θα συνδεθεί στο δίκτυο ώστε να περιορίζεται μόνο στις υπηρεσίες που του έχουν αποδοθεί.

2.1.7. Επιβάρυνση φορτίου (Traffic Overhead)

Σε κάθε τεχνολογία υπάρχει εξισορρόπηση των παραγόντων λειτουργίας της και τα VPN δε θα μπορούσαν να μην ακολουθούν τον κανόνα. Συγκεκριμένα τα αλληλοσυγκρουόμενα χαρακτηριστικά είναι η ευελιξία και ευχρηστία απέναντι στην ασφάλεια, η ταχύτητα απέναντι στην απόδοση της επικοινωνίας. Η επιβάρυνση αφορά είτε το κόστος που υπεισέρχεται από την κρυπτογράφηση των δεδομένων που μεταφράζεται στο πόση υπολογιστική ισχύς καταναλώνεται, είτε στο ποσό του παραπάνω εύρους ζώνης που απαιτείται για τη μετάδοση των μεγαλύτερου μεγέθους πακέτων που προκύπτουν μέσω encapsulation. Θα πρέπει λοιπόν το VPN να μπορεί να είναι ευέλικτο στη διαμόρφωσή του ώστε να καλύπτει τις διάφορες ανάγκες που θα προκύψουν κατά τη διάρκεια χρήσης του. Για παράδειγμα θα μπορούσε να γίνεται κατηγοριοποίηση των δεδομένων ανάλογα με την αξία του και έτσι άλλα να κρυπτογραφούνται, άλλα απλώς να πιστοποιούνται και άλλα να αποστέλλονται χωρίς να υποστούν καμία επεξεργασία.

2.1.8. Nonrepudiation

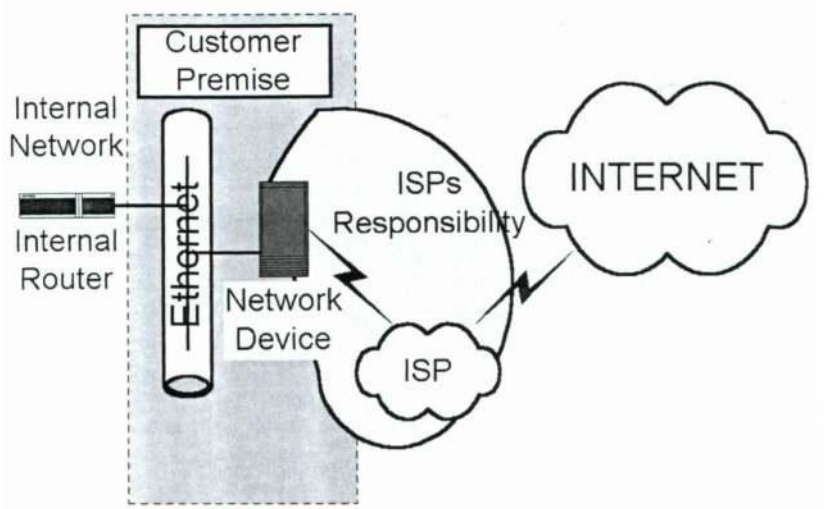
Ένα VPN πρέπει να έχει τη δυνατότητα θετικής αναγνώρισης ενός χρήστη χωρίς αυτός να μπορεί να αρνηθεί την αναγνώριση που έγινε. Η απαίτηση αυτή έχει μεγάλη σημασία για τις εφαρμογές του ηλεκτρονικού εμπορίου γιατί αν υπάρχει έστω και μια μικρή αμφιβολία για το ποιος έχει κάνει μια παραγγελία τότε αυτή δεν μπορεί να εκτελεστεί για ευνόητους λόγους. Η εξασφάλιση αυτής της ιδιότητας μπορεί να γίνει με χρήση digital signature.

2.2 VPN ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

Σε αυτή την ενότητα θα αναφερθούμε στις διάφορες αρχιτεκτονικές με τις οποίες μπορούμε να δημιουργήσουμε ένα VPN. Το ποια από αυτές τελικά θα επιλέξουμε εξαρτάται από πολλούς παράγοντες και πρώτα πρώτα από τις ανάγκες του οργανισμού που θέλει να εγκαταστήσει το VPN. Με άλλα λόγια πόσους χρήστες θα πρέπει αυτό να εξυπηρετεί και πόσο αναμένεται να αυξηθεί ο φόρτος στο μέλλον από την προσθήκη νέων χρηστών, πόση ανάγκη για ασφάλεια υπάρχει, για ποιους σκοπούς θα χρησιμοποιείται το VPN (π.χ. e-commerce) κ.α. Επίσης η επιλογή που θα κάνουμε θα εξαρτάται και από τις δυνατότητες του οργανισμού δηλαδή από την υποδομή σε hardware που αυτός έχει καθώς και από το πόσο και έως ποιο βαθμό μπορεί το τεχνικό του προσωπικό να υποστηρίξει κάποια λύση VPN η οποία θα επιλεγεί. Έτσι λοιπόν, με βάση την αρχιτεκτονική τους, μπορούμε να ξεχωρίσουμε τις ακόλουθες κατηγορίες VPN:

2.2.1. VPN υποστηριζόμενα από κάποιον Παροχέα Πρόσβασης στο Internet (ISP)

Αυτός είναι ο πιο απλός τρόπος να εγκαταστήσει ένας οργανισμός ένα Virtual Private Network. Απευθύνεται σε κάποιον ISP ο οποίος εγκαθιστά στο κτήριο του οργανισμού κάποια συσκευή δικτύωσης η οποία θα αναλάβει να δημιουργήσει τα tunnels που χρειάζονται για το VPN. Η συσκευή αυτή θα έχει κάποιο λειτουργικό σύστημα, όπως για παράδειγμα το Unix επειδή έτσι θα μπορεί κανείς να τη διαχειριστεί εξ αποστάσεως (remote managing). Επίσης πολύ πιθανή είναι και η χρησιμοποίηση κάποιου firewall μετά από τη συσκευή δικτύωσης. Ένα γενικό σχήμα αυτής της VPN αρχιτεκτονικής φαίνεται στο σχήμα 1(επόμενη σελίδα).



Σχήμα 1. VPN παρεχόμενο από ISP

Παρατηρούμε μία εταιρεία, με τη συγκεκριμένη VPN αρχιτεκτονική, έχει τη μικρότερη δυνατή εμπλοκή μιας και η συσκευή δικτύωσης αυτή καθεαυτή καθώς και η επικοινωνία της προς τα έξω αναλαμβάνονται εξ ολοκλήρου από τον Παροχέα Πρόσβασης στο Internet. Παρόλο που ο τρόπος αυτός φαίνεται να είναι ο πιο απλός αφού ο οργανισμός μετατρέπεται σε απλό χρήστη του VPN, αυτό δεν είναι απόλυτα σωστό.

Υπάρχει μία σειρά από προβλήματα τα οποία για να λυθούν απαιτούν επέμβαση από τη μεριά του χρήστη του VPN. Το πρώτο και κυριότερο είναι το θέμα της ασφάλειας. Είναι πολύ αμφίβολο το αν ο ISP θα είναι υπεύθυνος για την ασφάλεία παρόλο που είναι αυτός που «δίνει» τη συσκευή δικτύωσης και παρέχει τελικά το VPN. Οι ISPs είναι κατά πρώτο λόγο παροχείς πρόσβασης στο Internet και κατά δεύτερο παροχείς VPN υπηρεσιών. Έτσι λοιπόν αν κάποιος χρήστης δημιουργήσει, μέσω ενός VPN, κάποιο πρόβλημα ασφάλειας τότε είναι πολύ πιθανό ότι δεν θα εμποδιστεί από τον ISP. Στην περίπτωση αυτή θα πρέπει ο οργανισμός – χρήστης του VPN να προσλάβει μία εξωτερική ομάδα η οποία θα δημιουργήσει μία πολιτική ασφαλείας η οποία θα πρέπει στη συνέχεια να εφαρμοστεί από τον ISP.

Ένα άλλο πρόβλημα αφορά στο ποιος και πόσο γρήγορα μπορεί να αλλάξει την πολιτική πρόσβασης του VPN. Ο ISP μπορεί να μην έχει τον απαραίτητο χρόνο να κάνει τέτοιες αλλαγές. Έτσι κάποιος χρήστης μπορεί να ζητήσει να προσπελάσει κάποιο προορισμό ή κάποια υπηρεσία η οποία μέχρι εκείνη τη στιγμή δεν διατίθεται.

Στην περίπτωση αυτή θα χρειαστούν κάποιες μέρες για να εξασφαλισθούν οι απαραίτητες άδειες πρόσβασης και στη συνέχεια θα πρέπει να συμπληρωθούν κάποιες φόρμες οι οποίες θα ζητούν από τον ISP να αλλάξει το configuration του δικτύου. Είναι προφανές ότι η διαδικασία αυτή είναι αρκετά δύσκαμπτη και χρονοβόρα. Επίσης, επειδή για να προστεθεί κάποια καινούρια υπηρεσία, είναι πιθανό να χρειάζεται να γίνουν αρκετές αλλαγές στο configuration(διαμόρφωση) του VPN, θα πρέπει για κάθε αλλαγή να ενημερώνεται ο χρήστης αφενός ότι η αλλαγή έγινε και αφετέρου για τον τρόπο με τον οποίο αυτή έγινε.

Μεγάλη προσοχή θα πρέπει να δοθεί επίσης και στην περίπτωση του εντοπισμού και αντιμετώπισης των βλαβών. Αν προκύψει κάποια βλάβη τότε τα πράγματα μπορεί να γίνουν πολύ δύσκολα αν το τεχνικό προσωπικό του οργανισμού δεν έχει αντιμετωπίσει κάτι παρόμοιο. Μπορεί να χρειαστούν ακόμα και εβδομάδες ειδικά για προβλήματα τα οποία δεν είναι συνεχή, δηλαδή εμφανίζονται κατά διαστήματα και στη συνέχεια εξαφανίζονται. Για να προληφθούν τέτοιες περιπτώσεις είναι προτιμότερο κανείς να πληρώσει παραπάνω χρήματα σε κάποιον ISP έτσι ώστε να εξασφαλίσει υποστήριξη σε περιπτώσεις βλαβών.

Πολύ σημαντικό θέμα επίσης είναι και αυτό του authorization(εξουσιοδότηση), δηλαδή του ποιοι χρήστες επιτρέπεται να δημιουργήσουν ένα tunnel(δίοδος) προς το VPN κάποιου οργανισμού. Η βάση δεδομένων που χειρίζεται αυτή την πληροφορία θα βρίσκεται στην πλευρά του ISP ή στην πλευρά του χρήστη του VPN; Αυτό είναι πολύ σημαντικό στην περίπτωση που κάποιος υπάλληλος απολυθεί ή παραιτηθεί από τη θέση του. Καταλαβαίνουμε ότι θα θέλαμε άμεσα να μην του ξαναδώσουμε την ευκαιρία να χρησιμοποιήσει το δίκτυό μας κάτι το οποίο είναι ιδιαίτερα δύσκολο όταν δεν μπορούμε να προσπελάσουμε αυτές τις βάσεις γρήγορα. Θα πρέπει επίσης, με κάποιο τρόπο, ο οργανισμός που χρησιμοποιεί το VPN να μπορεί να παρακολουθεί τη χρησιμοποίηση του (utilization) καθώς και τη χρησιμοποίηση της συσκευής δικτύωσης. Έτσι μόνο θα μπορεί να ξέρει έγκαιρα πότε θα χρειαστεί να αναβαθμίσει κάποιο από τα δύο έτσι ώστε να μην δημιουργηθεί κάποιο πρόβλημα λόγω μεγάλου φόρτου.

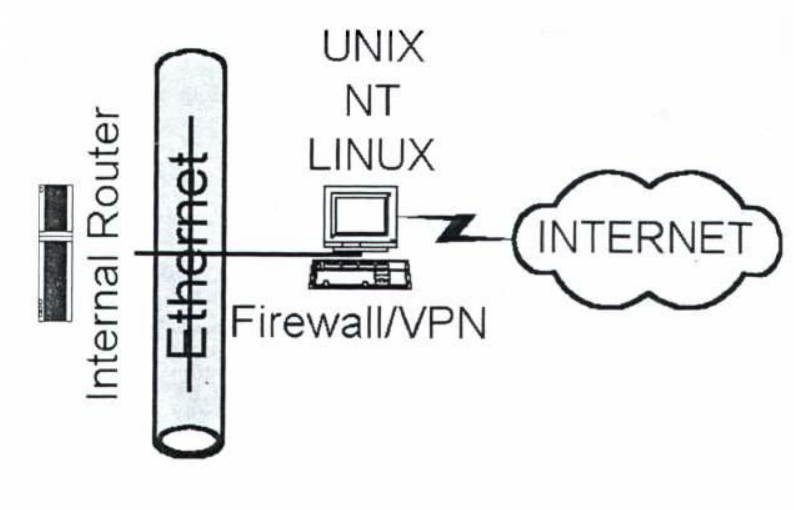
Ένα τελευταίο αλλά πολύ σημαντικό θέμα αφορά την ασφάλεια των κλειδιών. Θα πρέπει τα κλειδιά να

φυλάσσονται σε κάποιο «σίγουρο» μέρος όχι μόνο για λόγους ασφαλείας αλλά και για να ξέρει κανείς που μπορεί να τα βρει αν χρειαστεί κάποιο από αυτά. Για παράδειγμα τα κλειδιά κρυπτογράφησης μπορεί να χρειάζονταν στην περίπτωση που η συσκευή δικτύωσης χαλάσει και πρέπει να αντικατασταθεί. Συνήθως σε τέτοιες περιπτώσεις ακυρώνονται τα παλιά κλειδιά και δημιουργούνται καινούρια. Για να μπορέσουμε όμως να τα ακυρώσουμε θα πρέπει να τα γνωρίζουμε και άρα να τα επαναφέρουμε από κάποιο ασφαλές μέρος στο οποίο τα έχουμε κρατήσει.

2.2.2 VPN βασισμένα σε Πύρινο τείχος Firewalls (Firewall-Based VPN)

Τα VPN τα οποία βασίζονται σε Firewalls είναι ίσως ο πιο διαδεδομένος τύπος VPN. Αυτό δεν σημαίνει βέβαια ότι αυτού του τύπου τα VPN υπερτερούν σε σχέση με τα υπόλοιπα, απλά οι περισσότεροι οργανισμοί που αυτή τη στιγμή είναι συνδεδεμένοι στο Internet διαθέτουν firewalls, με αποτέλεσμα το μόνο που χρειάζεται από την πλευρά τους είναι να προσθέσουν το κατάλληλο λογισμικό που θα κάνει το encryption(κρυπτογράφηση). Μάλιστα αν κάποια εταιρεία ή οργανισμός διαθέτει κάποιο πρόσφατα αγορασμένο firewall, τότε είναι πολύ πιθανό αυτό να έχει ενσωματωμένη τη δυνατότητα να πραγματοποιεί κάποιο VPN encryption.

Μεγάλη σημασία από άποψη ασφάλειας πρέπει να δώσει κανείς στο λειτουργικό σύστημα του firewall και πιο συγκεκριμένα στα τρωτά σημεία που πιθανώς αυτό να έχει. Κανένα σύστημα δεν είναι εκατό τοις εκατό ασφαλές και έτσι, αν θέλουμε να δημιουργήσουμε ένα VPN θα πρέπει το λειτουργικό σύστημα της συσκευής δικτύωσης να είναι όσο το δυνατόν ασφαλέστερο. Στο σχήμα 2 φαίνεται ένα firewall-based VPN. Σημειώνουμε εδώ και πάλι ότι η υλοποίηση ενός τέτοιου τύπου VPN δεν είναι απλή, αλλά βολεύει πολύ τις εταιρείες οι οποίες διαθέτουν ήδη τέτοιες συσκευές.



Σχήμα 2. VPN βασισμένο σε Firewall

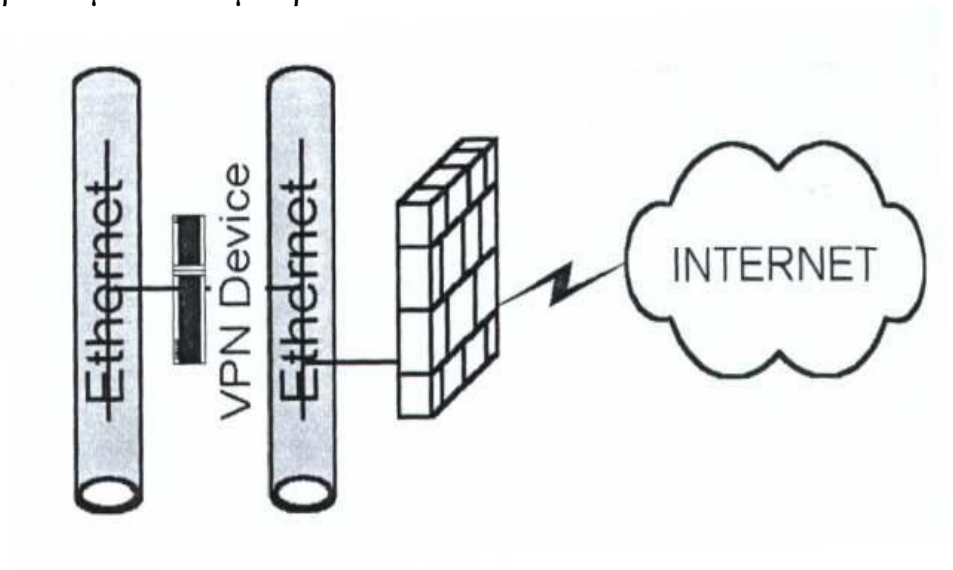
Θα πρέπει τέλος να διευκρινίσουμε το εξής: υπάρχουν τρία ήδη firewalls στην αγορά: τα stateful-inspection, τα proxy(πληρεξουσιότητα) και τα packet filtering(φιλτράρισμα πακέτων). Μιλώντας για προσθήκη VPN τεχνολογίας σε ένα firewall αναφερόμαστε στον πρώτο από τους τρεις τύπους. Αυτός «τρέχει» στα επίπεδα 2 και 3 του OSI protocol stack(πρωτόκολλο στοίβας). Ένας proxy server τρέχει στο επίπεδο εφαρμογών ενώ ο packet filtering πρέπει να ελέγχει το πλήρες πακέτο που περνάει κάθε στιγμή. Επειδή όμως όσο κατεβαίνουμε πιο χαμηλά στα επίπεδα του protocol stack τόση μεγαλύτερη ασφάλεια μπορούμε να πετύχουμε, όταν μιλάμε για προσθήκη VPN τεχνολογίας, αναφερόμαστε πάντα στα stateful-inspection firewalls τα οποία τρέχουν σε επίπεδα χαμηλότερα από τα υπόλοιπα.

2.2.3 VPN βασισμένα σε μαύρα κουτιά (Black-Box Based)

Στην περίπτωση αυτή, ο παροχέας VPN υπηρεσιών προσφέρει ακριβώς αυτό, ένα μαύρο κουτί, δηλαδή μία συσκευή με το απαραίτητο λογισμικό για να δημιουργήσουμε ένα tunnel. Μερικές από τις συσκευές αυτές συνοδεύονται από software(λογισμικό) το οποίο τρέχει σε κάποιον υπολογιστή και μας βοηθάει να τις διαχειριστούμε ενώ σε άλλες μπορούμε να αλλάξουμε configuration(ρυθμίσεις) μέσω Web. Στην περίπτωση των black boxes(μαύρα κούτια) χρειαζόμαστε τις περισσότερες φορές έναν ακόμα server για να κάνουμε το

authentication(ταυτοποίηση) των χρηστών. Παρά το γεγονός αυτό, ένα ελκυστικό χαρακτηριστικό που έχουν τα black boxes είναι ότι το λογισμικό τους επιτρέπει για το authentication να χρησιμοποιείται μία ήδη υπάρχουσα βάση δεδομένων, η οποία βρίσκεται σε κάποιον server και έτσι απαλλασσόμαστε από το πρόβλημα του να έχουμε διάφορες βάσεις με χρήστες και να προσπαθούμε να τις κρατάμε συγχρονισμένες.

Τις περισσότερες φορές μαζί με τα black boxes χρειαζόμαστε και κάποιο firewall αν και οι περισσότεροι κατασκευαστές τέτοιων συσκευών έχουν αρχίσει να ενσωματώνουν δυνατότητες firewall σε αυτά. Το firewall παρέχει ασφάλεια στην επιχείρηση ενώ το VPN ασφάλεια στα δεδομένα. Το μόνο που θα πρέπει να εξασφαλίσουμε σε αυτή την περίπτωση είναι ότι τα encrypted πακέτα θα μπορούν να περνούν από το firewall. Στο σχήμα 3 φαίνεται το διάγραμμα ενός VPN βασισμένου σε μαύρο κουτί.



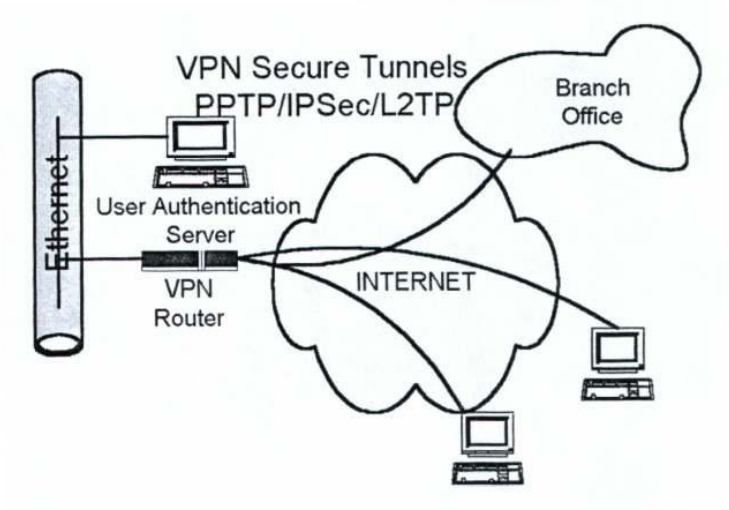
Σχήμα 3. VPN βασισμένο σε μαύρο κουτί

2.2.4. VPN βασισμένα σε Routers (Router-Based)

Ο τύπος αυτός των VPN ταιριάζει σε οργανισμούς οι οποίοι έχουν επενδύσει αρκετά χρήματα σε routers και έχουν τεχνικό προσωπικό εξειδικευμένο σε αυτούς. Υπάρχουν δύο τύποι τέτοιων VPN. Στον πρώτο γίνεται στον router εγκατάσταση λογισμικού που κάνει encryption ενώ ο δεύτερος χρησιμοποιεί για τον ίδιο λόγο

μια κάρτα από έναν τρίτο κατασκευαστή, η οποία τοποθετείται στο σασί του router(δρομολογήτης) με αποτέλεσμα να αποδεσμεύεται η CPU(επεξεργαστής) από το φόρτο του encryption. Αυτό είναι πολύ σημαντικό αφού η διαδικασία του routing απαιτεί αρκετούς πόρους, ειδικά όταν τα routes είναι πολλά και ο routing αλγόριθμος intensive(εντατικός).

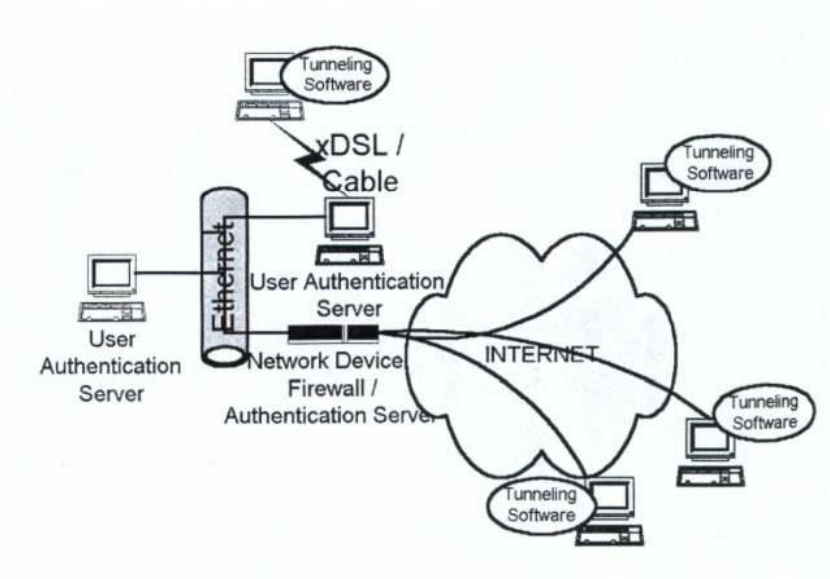
Επίσης ένα άλλο ζήτημα στα VPN αυτού του τύπου είναι αν ο router θα χειρίζεται το authentication των χρηστών ή αν θα πρέπει να συνεργάζεται με κάποια άλλη συσκευή που θα κάνει αυτή τη δουλειά. Στο σχήμα 4 φαίνεται ένα VPN βασισμένο σε router το οποίο απαιτεί και κάποιον server για το authentication.



Σχήμα 4.VPN βασισμένο σε router

2.2.5. VPN βασισμένα σε πρόσβαση από απόσταση (Remote Access-Based)

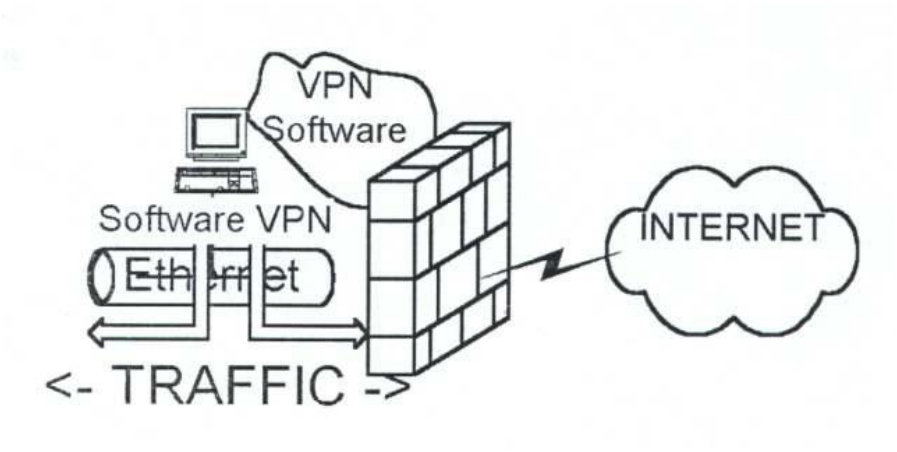
Όπως φανερώνει και το όνομά τους, αυτού του είδους τα Virtual Private Networks, έχουν να κάνουν με χρήστες οι οποίοι βρίσκονται κάπου εκτός της επιχείρησης και προσπαθούν με τη βοήθεια software να δημιουργήσουν ένα tunnel προς κάποια συσκευή δικτύου η οποία επιτρέπει τη σύνδεση. Το tunnel αυτό μπορεί να δημιουργηθεί μέσω Internet αλλά και μέσω μίας dial-up ή ISDN γραμμής ή και ενός X.25 δικτύου. Ένα τέτοιο σενάριο φαίνεται στο σχήμα 5(επόμενη σελίδα).



Σχήμα 5. VPN βασισμένο σε πρόσβαση από απόσταση

2.2.6 VPN βασισμένα στο λογισμικό (Software-based)

Είναι ο τελευταίος τύπος VPN αρχιτεκτονικής με τον οποίο θα ασχοληθούμε. Εδώ χρησιμοποιείται λογισμικό για να γίνει tunneling ή encryption από κάποιον πελάτη προς κάποιον εξυπηρετητή (client - server). Η διαφορά από τους υπόλοιπους τύπους έγκειται στο γεγονός ότι αντί να έχουμε ένα μοναδικό σημείο πρόσβασης προς το εσωτερικό δίκτυο ενός οργανισμού (π.χ. firewall) και μέσα στο δίκτυο αυτό η πληροφορία να είναι αποκωδικοποιημένη (decrypted), εδώ κάθε σταθμός του εσωτερικού δικτύου μπορεί να έχει ένα δικό του ζευγάρι ιδιωτικού - δημόσιου κλειδιού και η πληροφορία να φτάνει σε αυτόν κρυπτογραφημένη. Φυσικά και σε αυτή την περίπτωση θα πρέπει να φροντίσουμε έτσι ώστε αν υπάρχει κάποιο firewall που δεν παίζει το ρόλο VPN συσκευής, να μπορεί να περνάει μέσα από αυτό η κρυπτογραφημένη πληροφορία. Το σχήμα 6(επόμενη σελίδα) δείχνει έναν τέτοιο τύπο VPN.



Σχήμα 6. VPN βασισμένο σε λογισμικό

2.3 Βασικές Τοπολογίες VPN

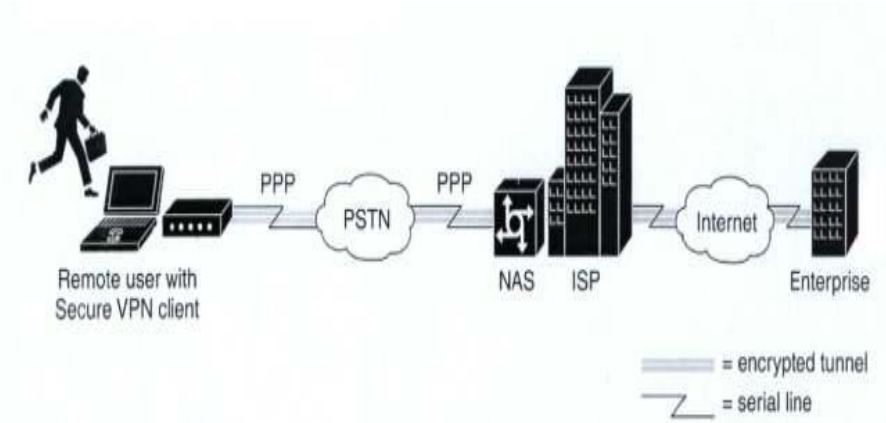
Στο κεφάλαιο αυτό θα ασχοληθούμε με τις διάφορες τοπολογίες των Virtual Private Networks που μπορούμε να έχουμε. Οι πιο βασικές από αυτές είναι: Remote Access VPN, Intranet VPN, Extranet VPN και Intracompany VPN. Τα VPN της τελευταίας κατηγορίας δεν είναι ακόμα πολύ διαδεδομένα.

2.3.1. Remote Access VPN (Απομακρυσμένη σύνδεση)

Ένα VPN αυτής της κατηγορίας εξυπηρετεί remote mobile χρήστες. Συγκεκριμένα παρέχει τη δυνατότητα σύνδεσης αυτού του τύπου χρηστών με τα κεντρικά γραφεία της εταιρείας μέσω ενός tunnel κρυπτογράφησης δεδομένων. Η δημιουργία του τελευταίου μπορεί να γίνει με ειδικό λογισμικό εγκατεστημένο στον εξοπλισμό του χρήστη. Στην άλλη άκρη του tunnel υπάρχει μια οντότητα που αποτελεί είσοδο στο ιδιωτικό δίκτυο της εταιρείας που μπορεί να είναι και αυτό ένα VPN.
Τα remote access VPN χωρίζονται σε δύο κατηγορίες: στα client-initiated και στα network access server (NAS)-initiated.

2.3.2. Client initiated(έναρξη σύνδεσης από πελάτη)

Στην περίπτωση αυτή, απομακρυσμένοι χρήστες χρησιμοποιούν client εφαρμογές για να δημιουργήσουν κρυπτογραφημένα IP tunnels, μέσω του shared(διαμοιράσιμου) δικτύου ενός ISP(παροχέα), προς το δίκτυο κάποιας εταιρείας. Το πλεονέκτημα των client-initiated VPN έναντι των NAS-initiated είναι ότι χρησιμοποιούν κρυπτογραφημένο tunneling για τη σύνδεση μεταξύ της client εφαρμογής και του ISP μέσω του δημόσιου τηλεφωνικού δικτύου (PSTN).



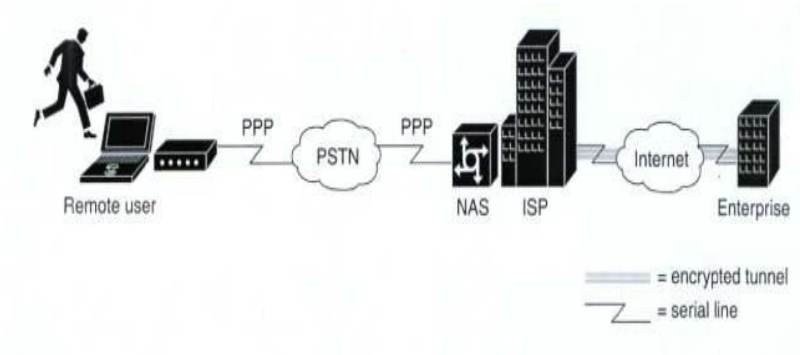
Σχήμα 1. Client-initiated remote access VPN

Στο σχήμα 1 φαίνεται ένα client-initiated remote access VPN. Η client εφαρμογή δημιουργεί μία PPP σύνδεση με το NAS του ISP και εν συνεχεία σχηματίζεται ένα κρυπτογραφημένο tunnel μέσω του Δημόσιου τηλεφωνικού δικτύου.

2.3.3. NAS-initiated(έναρξη σύνδεσης από τον εξυπηρετητή):

Στην περίπτωση αυτή οι απομακρυσμένοι χρήστες κάνουν μία κλήση στο Network Access Server του ISP και αυτό δημιουργεί ένα κρυπτογραφημένο tunnel με το VPN της εταιρείας. Τα NAS-initiated VPN δίνουν τη

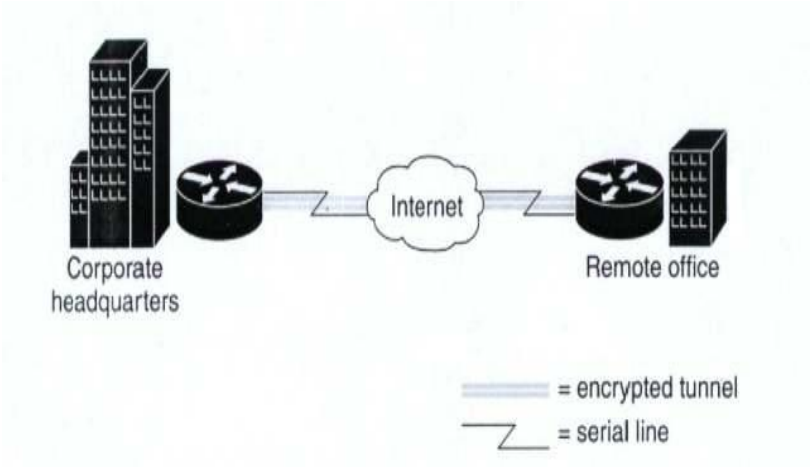
δυνατότητα στους χρήστες να συνδεθούν σε διάφορα δίκτυα χρησιμοποιώντας πολλαπλά tunnels, ενώ η client εφαρμογή δεν χρειάζεται να έχει λογισμικό για τη δημιουργία tunnels. Το αρνητικό στην περίπτωση αυτή είναι ότι η σύνδεση μεταξύ του χρήστη και του ISP δεν είναι κρυπτογραφημένη και άρα στηρίζεται στο PSTN, το οποίο δυστυχώς δεν παρέχει καμία ασφάλεια. Το διάγραμμα ενός τέτοιου VPN φαίνεται στο σχήμα 2.



Σχήμα 2. NAS-initiated remote access VPN

2.3.4. Εσωτερικό δίκτυο vpn(intranet vpn)

Ένα intranet είναι ένα δίκτυο εργασίας το οποίο είναι εσωτερικό σε κάποια εταιρεία. Παρέχει τις πιο πρόσφατες πληροφορίες και υπηρεσίες σε όλους τους υπαλλήλους της εταιρείας που συνδέονται σε αυτό. Τα intranet προσφέρουν ένα κοινό, ανεξάρτητο πλατφόρμας interface(διασύνδεσης), το οποίο είναι λιγότερο ακριβό στην υλοποίηση από μία client/server εφαρμογή. Επιπλέον τα Intranet αυξάνουν την παραγωγικότητα των υπαλλήλων επιτρέποντας μία reliable(αξιόπιστη) σύνδεση σε consistent(λογικές) πληροφορίες. Τα Intranet VPN επιτρέπουν την ίδια ασφάλεια και διασυνδεσιμότητα μεταξύ των κεντρικών γραφείων μιας εταιρείας και απομακρυσμένων γραφείων.

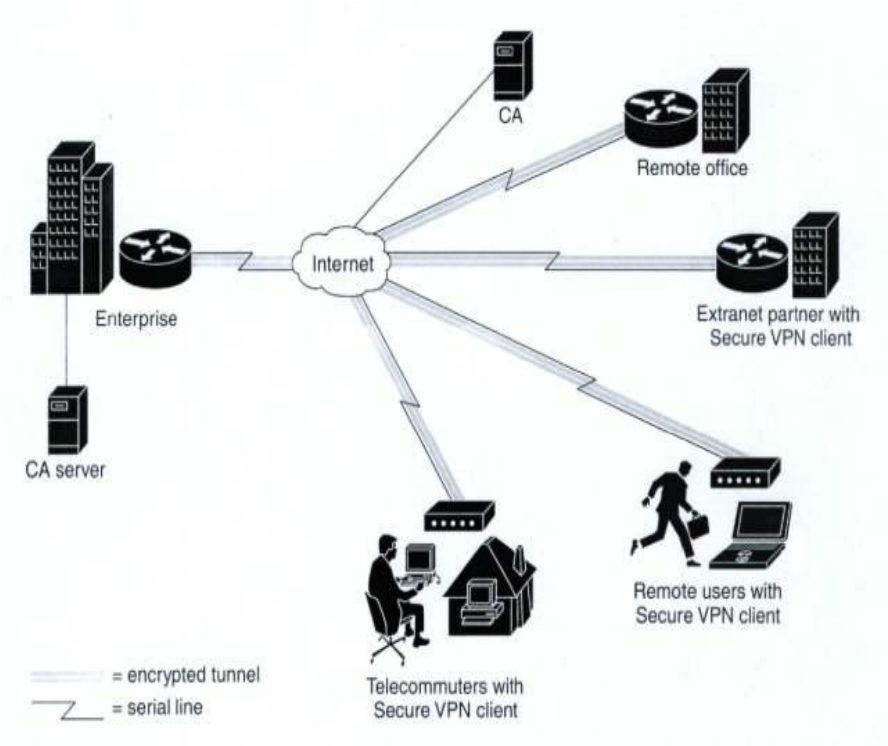


Σχήμα 3. Intranet VPN

2.3.5. Εξωτερικό δίκτυο vpn(extranet vpn)

Το extranet είναι ένα intranet το οποίο επιτρέπει και κάποια περιορισμένη πρόσβαση σε πελάτες, προμηθευτές και συνεργάτες της εταιρείας. Τα extranets διαφέρουν από τα intranets στο ότι επιτρέπουν πρόσβαση και σε χρήστες που δεν είναι υπάλληλοι της εταιρείας είτε μέσω χρήσης του HTTP πρωτοκόλλου είτε μέσω κάποιου πρωτοκόλλου στο οποίο θα συμφωνούν οι συμβαλλόμενοι στην επικοινωνία φορείς. Το πεδίο στο οποίο θα εξαπλωθούν ευρέως τα VPN της κατηγορίας είναι το ηλεκτρονικό εμπόριο στη γενική του μορφή, καθώς οι εταιρείες αποκτούν τη δυνατότητα ασφαλούς, γρήγορης και αποτελεσματικής εκτέλεσης συναλλαγών με τους εμπορικούς τους συνεργάτες. Επιτρέποντας μεγαλύτερη πρόσβαση στα resources(πηγές) τους, οι εταιρείες με extranet VPN βελτιώνουν την εικόνα τους στους πελάτες τους, μειώνοντας ταυτόχρονα τα έξοδά τους.

Στο σχήμα 4 φαίνεται μία extranet VPN τοπολογία. Χρησιμοποιώντας digital certificates(ψηφιακές πιστοποιήσεις), οι clients δημιουργούν μέσω Internet, ασφαλή tunnels προς το δίκτυο μίας εταιρείας. Κάθε client λαμβάνει από το Certification Authority (Αρχή πιστοποίησης) ένα digital certificate το οποίο χρησιμοποιείται για authentication από τον CA server της εταιρείας.

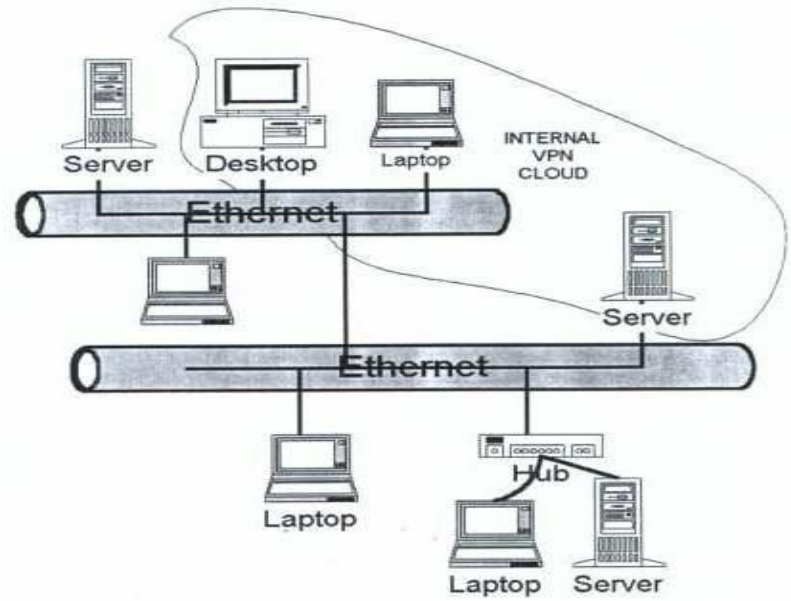


Σχήμα 4.Extranet VPN

2.3.6. Ενδοεταιρικό VPN (Intracompany VPN)

Η χρήση τέτοιων VPN δεν έχει διαδοθεί ακόμη αλλά υπάρχουν διάφοροι λόγοι που θα οδηγήσουν στην εξάπλωσή τους. Η βασική ιδέα πίσω από τη χρήση τους είναι η δημιουργία ενός VPN μέσα στο δίκτυο της εταιρείας, το οποίο μπορεί να είναι ένα VPN, που θα προσφέρει προστασία σε πολύτιμους πόρους και πληροφορίες σημαντικής αξίας για την εταιρεία. Τέτοιες πληροφορίες μπορεί να είναι στοιχεία ερευνών πάνω σε νέα προϊόντα, οικονομικά στοιχεία, πολιτικές παραγωγής και προώθησης προϊόντων, κλπ. Βασική αιτία χρήσης τους είναι το γεγονός ότι πολλές παραβιάσεις στα δίκτυα εταιρειών γίνονται από τους ίδιους τους υπαλλήλους της, οι οποίοι έχουν αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες περιοχές. Οι απώλειες από τέτοιου είδους επιθέσεις δικαιολογούν την υλοποίηση τέτοιων

λύσεων. Το παρακάτω σχήμα δείχνει μια απλή περίπτωση εφαρμογής ενός intracompany VPN, όπου ένας αριθμός συσκευών έχει συνδεθεί με τέτοιο τρόπο ώστε να αποτελεί ένα εσωτερικό VPN. Όπως φαίνεται οι συσκευές του VPN μπορεί να μην ανήκουν στο ίδιο υποδίκτυο, πράγμα που αποτελεί χαρακτηριστικό της τεχνολογίας αυτής.



Σχήμα 5. Intracompany VPN

2.4 Πλεονεκτήματα και μειονεκτήματα vpn

2.4.1. Πλεονεκτήματα VPN

Η χρήση VPN αποφέρει σημαντικά οφέλη σε όλα τα μέρη που συμμετέχουν, είτε αυτά αποτελούν την εταιρεία που το χρησιμοποιεί, είτε τον τελικό χρήστη του VPN, είτε τον ISP που παρέχει την υποδομή. Σε γενικές γραμμές τα οφέλη περιλαμβάνουν μείωση των δαπανών για τις τηλεπικοινωνίες, καλύτερη διαχείριση και ευκολότερη συντήρηση, πιο εύκολη κατασκευή του συστήματος.

2.4.1.1 Άμεσα οικονομικά οφέλη

Είναι δυνατό να επιτευχθεί σημαντική μείωση στο συνολικό κόστος που θα επιβαρύνει την εταιρεία αν και το ακριβές ποσοστό θα προκύψει από τον συμψηφισμό του ποσού που η εταιρεία κερδίζει και του ποσού που χρειάζεται για να υλοποιήσει και να συντηρεί το VPN. Έτσι, αν η εταιρεία χρησιμοποιούσε ένα ιδιωτικό δίκτυο, με τη χρήση VPN μπορεί να σταματήσει τη μίσθωση γραμμών, να μειώσει το κόστος από κλήσεις μεγάλων αποστάσεων που γίνονται από απομακρυσμένους χρήστες. Μπορεί επίσης να αφαιρέσει τον εξοπλισμό απομακρυσμένης πρόσβασης και παράλληλα όλο τον εξοπλισμό που τον υποστηρίζει (π.χ. UPS) και να μειώσει με αυτό τον τρόπο το προσωπικό που κάνει τη διαχείριση και τη συντήρηση του δικτύου της.

2.4.1.2 Σχεδιασμός δικτύου

Η τεχνολογία των VPN αποφέρει μεγάλα οφέλη στον τομέα σχεδιασμού του δικτύου του οργανισμού. Ο οργανισμός δεν είναι επιφορτισμένος με το σχεδιασμό ενός πολύπλοκου WAN, την εύρεση των αναγκαίων επιδόσεων των συνδέσεων μεταξύ των περιοχών ενδιαφέροντος και υπολογισμό του απαιτούμενου εύρους

ζώνης. Το κύριο ενδιαφέρον του είναι να εξασφαλίσει μια καλή σύνδεση με τον ISP. Πριν την εμφάνιση του Internet ο οργανισμός έπρεπε να εγκαταστήσει έναν αριθμό μισθωμένων γραμμών για να συνδέσει τα διάφορα γραφεία του.

Τα θέματα που έπρεπε να ληφθούν υπόψη από τον σχεδιαστή του δικτύου ήταν:

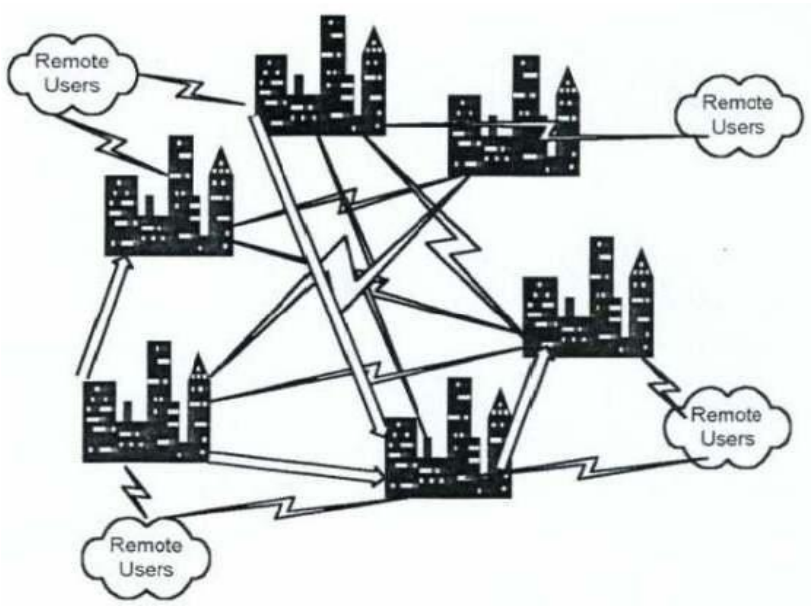
→ Η χρήση βοηθητικών (backup) γραμμών για να αντιμετωπιστούν περιπτώσεις μη λειτουργίας κάποιων από τις κύριες,

→ Η δυνατότητα επέκτασής του,

→ Η παροχή πρόσβασης σε απομακρυσμένους χρήστες και

→ Ο καθορισμός του μεγέθους της κυκλοφορίας μέσα στο δίκτυο.

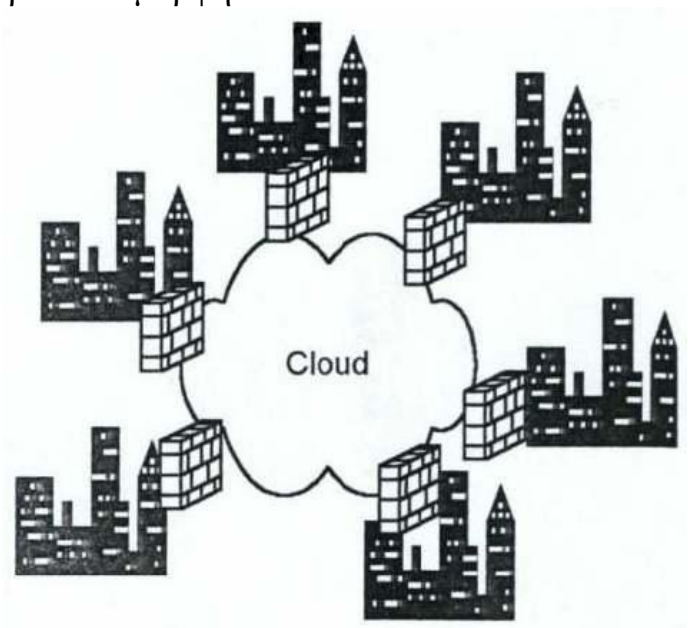
Ένα ιδιωτικό δίκτυο που θα υλοποιούνταν με μέσα της εταιρείας θα είχε τη γενική μορφή του παρακάτω σχήματος.



Σχήμα 1. Μορφή ιδιωτικού δικτύου

Η χρήση ενός VPN μειώνει όλη αυτή την εργασία, καθώς ο ISP είναι αυτός που αναλαμβάνει την μεταφορά των δεδομένων. Έτσι το WAN μπορεί να είναι επεκτάσιμο και βασισμένο πάνω σε ένα πρωτόκολλο. Ο ISP επίσης έχει αναλάβει και τα θέματα που αφορούν πλεονασμό συνδέσεων ώστε να εξασφαλίζεται η αξιοπιστία του δικτύου. Ο οργανισμός πρέπει να

καθορίσει το μέγεθος της σύνδεσης με τον ISP που συνεπάγεται μελέτη της κίνησης μέσα στο εσωτερικό δίκτυο κάθε περιοχής και υπολογισμό του ποσοστού που θα διακινείται μέσω Internet. Το αποτέλεσμα της αυτής της μεταφοράς του σχεδιασμού στον ISP έχει ως αποτέλεσμα το ιδιωτικό δίκτυο της εταιρείας να αποκτά την παρακάτω μορφή.



Σχήμα 2.Μορφή ιδιωτικού δικτύου με χρήση ISP.

2.4.1.3 Κεντρικοποιημένος έλεγχος

Αρκετοί κατασκευαστές υποστηρίζουν κεντρικοποιημένο έλεγχο των VPN προϊόντων τους, κάτι το οποίο είναι ένας καλός μηχανισμός ανίχνευσης βλαβών αλλά και ένα χαρακτηριστικό που προσφέρει μεγαλύτερη ασφάλεια. Αν υποθέσουμε ότι έχει παρουσιαστεί ένα πρόβλημα σύνδεσης μεταξύ μιας εφαρμογής πελάτη σε ένα τμήμα και ενός εξυπηρετητή σε ένα άλλο τμήμα τότε θα έπρεπε να γίνει συντονισμός του προσωπικού των δύο αυτών τμημάτων για να επιλυθεί το πρόβλημα. Τα πράγματα περιπλέκονται όταν κάποιες λύσεις δεν αποδίδουν και αναγκαστικά στρεφόμαστε στον κατασκευαστή με αποτέλεσμα να καθυστερεί η επίλυση του προβλήματος. Η χρήση κεντρικοποιημένου ελέγχου δεν απαιτεί τέτοια αντιμετώπιση αλλά το μόνο που χρειάζεται είναι ο χρήστης που έχει το πρόβλημα και ένας τεχνικός να είναι

on-line και με παρακολούθηση των δύο άκρων του VPN μπορεί να απομονωθεί η αιτία του. Παράλληλα η ίδια προσέγγιση μπορεί να εφαρμοστεί στη συντήρηση του VPN. Σε περίπτωση που δεν υπάρχει κεντρικοποιημένος έλεγχος μπορεί να γίνει εγκατάσταση modem με κρυπτογραφικές ιδιότητες σε κάθε κονσόλα συσκευής του VPN και έτσι να μπορεί με ειδικό λογισμικό να γίνεται διαχείρισή της.

2.4.1.4 Ευκολίες στον τελικό χρήστη

Ο χρήστης όταν θέλει να συνδεθεί με κάποιον εξυπηρετητή της χρειάζεται μόνο να πληρώνει το κόστος μιας τοπικής κλήσης συν μια μηνιαία συνδρομή στην περίπτωση που το VPN έχει υλοποιηθεί στο Internet. Έτσι υπάρχει σημαντική μείωση του κόστους. Παράλληλα μπορεί πολύ εύκολα να αποκτήσει οποιοδήποτε υλικό κρίνει αναγκαίο για να εξασφαλίσει μια συναλλαγή με κάποιον πελάτη. Το μόνο που πρέπει να κάνει είναι να συνδεθεί με κάποιον εξυπηρετητή της εταιρείας και να κατεβάσει το υλικό αυτό. Επίσης μπορεί να ανήκει σε κάποια κλάση προτεραιότητας οπότε και να μπορεί να εξυπηρετείται πιο γρήγορα. Η κατηγοριοποίηση των χρηστών αλλά και της διακινούμενης πληροφορίας μπορεί να βελτιώσει τη συμπεριφορά του δικτύου, αφού θα γίνεται ορθότερη χρήση των πόρων του, και να κάνει αποδοτική την εκτέλεση των διαφόρων υπηρεσιών που ζητούν οι τελικοί χρήστες.

2.4.1.5 Σύνδεση σε παγκόσμια βάση (Global reach)

Το Internet παρέχει σύνδεση σε παγκόσμια βάση καθώς ο κάθε χρήστης μπορεί να συνδεθεί με την εταιρεία του με τη βοήθεια κάποιου ISP. Διευκολύνεται σημαντικά η επέκταση της παρουσίας του οργανισμού ανά την υφήλιο που σημαίνει ότι μπορεί πιο εύκολα να προωθήσει τα προϊόντα του. Ακόμη και για εταιρείες με μικρό προϋπολογισμό η χρήση του Internet μπορεί να προσφέρει μια αγορά της τάξεως των εκατομμυρίων πελατών.

2.4.1.6. Νέοι τομείς δραστηριοποίησης των ISP

Οι ISP μπορούν με τη χρήση των VPN να προσφέρουν στους πελάτες τους οποιεσδήποτε υπηρεσίες τους ζητηθούν. Ακόμη και εφαρμογές τηλεδιάσκεψης μεταξύ κεντρικών πόλεων του πλανήτη είναι εφικτές. Αν ένας ISP μπορεί να προσφέρει και ένα βαθμό Quality of Service για τέτοιες εφαρμογές κάποιου οργανισμού τότε αυτόματα γίνεται στρατηγικός συνεργάτης και ταυτόχρονα ισχυροποιεί τη θέση του στην αγορά υπηρεσιών. Ο τομέας διαχείρισης των VPN θα γνωρίσει μεγάλη ανάπτυξη στο μέλλον καθώς οι τεχνολογίες δικτύωσης αναπτύσσονται με ρυθμούς που είναι πολύ γρήγοροι για να τους παρακολουθήσει το προσωπικό ενός οργανισμού. Επίσης τα θέματα ασφαλείας αποκτούν ιδιαίτερη σημασία ώστε πολλοί χρήστες VPN θα οδηγηθούν στην απόφαση χρησιμοποίησης ISP με εμπειρία στο συγκεκριμένο τομέα.

2.4.1.7 Προσφορά στρατηγικού πλεονεκτήματος

Η χρήση του Internet μέσω VPN προσφέρει στρατηγικό πλεονέκτημα σε κάθε οργανισμό. Η περαιτέρω αύξηση αυτής της κατηγορίας χρηστών θα οδηγήσει σε βελτίωση των προσφερόμενων υπηρεσιών καθώς κάθε οργανισμός θα απαιτεί νέες υπηρεσίες που θα τον φέρουν σε μια θέση ισχύος απέναντι στους υπολοίπους. Θα υπάρξει βελτίωση σε θέματα αξιοπιστίας και απόδοσης από πλευράς χρονικής καθυστέρησης.

2.4.2 Μειονεκτήματα των VPN

Η χρήση VPN παρουσιάζει κάποια μειονεκτήματα που αφορούν κυρίως τον τομέα της ασφάλειας. Το κύριο πρόβλημα που παρουσιάζεται είναι το ποιοι αλγόριθμοι κρυπτογράφησης μπορεί να χρησιμοποιηθούν καθώς η ομοσπονδιακή κυβέρνηση των Ηνωμένων Πολιτειών

τους θεωρεί ως εξειδικευμένα "πυρομαχικά". Έτσι επιβάλλει περιορισμούς στη χρήση τους εκτός των συνόρων τους με αποτέλεσμα να υπονομεύεται σημαντικά η ασφάλεια των VPN. Υπάρχουν προορισμοί όπου απαγορεύεται η χρήση οποιασδήποτε κωδικοποίησης με αποτέλεσμα η εκάστοτε εταιρεία να βρίσκεται στο δίλημμα να εγκαταστήσει μια ευάλωτη μορφή του δικτύου που ενδεχομένως να προκαλέσει γενικότερα προβλήματα ασφαλείας ή να αγνοήσει την αγορά της συγκεκριμένης περιοχής και να χάσει τα οποιαδήποτε οικονομικά οφέλη που μπορεί να αποκομίσει.

Η χρήση του Internet βάζει και κάποιους περιορισμούς σε θέματα απόδοσης των VPN. Απαιτητικές εφαρμογές όπως είναι η τηλεδιάσκεψη δεν μπορούν να εφαρμοστούν για κάθε τελικό χρήστη ενός VPN γιατί δεν πληρούνται οι απαιτήσεις απόδοσης του δικτύου. Επίσης εφαρμογές που αποτελούν απόκριση πραγματικού χρόνου δεν έχουν όφελος από χρήση VPN καθώς εκτός από την καθυστέρηση του Internet υπεισέρχεται και η καθυστέρηση κρυπτογράφησης των δεδομένων.

2.4.2.1 Κόστος ενός VPN

Το κόστος εγκατάστασης και χρήσης ενός VPN εκτείνεται πάνω σε διάφορους τομείς, μερικοί από τους οποίους είναι αυτοί που αποκομίζουν σημαντικά οφέλη από τα VPN. Συγκεκριμένα παρά το γεγονός ότι παρέχεται εύκολη πρόσβαση μέσω του Internet μπορεί το κόστος σύνδεσης με αυτό να είναι σημαντικό για κάποιους απομακρυσμένους χρήστες καθώς μπορεί να κάνουν κλήση μεγάλης απόστασης. Έτσι ίσως θα απαιτείται από τον οργανισμό η παροχή κάποιων γραμμών μηδενικής χρέωσης (0800). Επίσης οι ανάγκες διαχείρισης του VPN μπορεί να απαιτούν ειδικά modem που θα μπορούν να ελέγχουν κάθε συσκευή του.

Το σημαντικότερο κόστος που υπεισέρχεται είναι ο σχεδιασμός του. Όπως αναφέρθηκε, αυτός περνά στα χέρια του ISP, ο οποίος αναλαμβάνει τη μελέτη της κυκλοφορίας του δικτύου της εταιρείας και προσπαθεί να φτάσει σε ένα αποτέλεσμα που θα ικανοποιεί και τις απαιτήσεις για περαιτέρω υπηρεσίες, όπως αυτές ορίζονται στο SLA. Παράλληλα η εταιρεία πρέπει να λάβει σοβαρά υπόψη την ύπαρξη δευτερεύουσας

σύνδεσης με το Internet, ώστε να μπορεί να έχει κάποιες εναλλακτικές επιλογές σε περίπτωση που η κύρια σύνδεση παρουσιάζει προβλήματα. Το κόστος μιας ενδεχόμενης απομόνωσης από το παγκόσμιο δίκτυο μπορεί να είναι μεγαλύτερο σε σχέση με αυτό που απαιτείται για τη συντήρηση της σύνδεσης αυτής. Ένας άλλος παράγοντας είναι η ύπαρξη πλεονασμού στις συνδέσεις του ISP με άλλους ISP καθώς έτσι μπορεί να βελτιωθεί η αξιοπιστία της επικοινωνίας.

Η απόκτηση του εξοπλισμού VPN και των αδειών χρήσης του λογισμικού είναι ένας ακόμη παράγοντας που προστίθεται στο κόστος του VPN. Πρέπει να υπάρχουν οι συσκευές που θα κάνουν πιστοποίηση των χρηστών καθώς και οι συσκευές που θα επιτρέπουν πρόσβαση σε remote χρήστες με ασφάλεια.

Τέλος ένας παράγοντας κόστους είναι η ανάγκη συντήρησης και διαχείρισης του δικτύου. Η συντήρηση αφορά αναβάθμιση συσκευών ή λογισμικού που προσδίδουν νέες δυνατότητες στο VPN. Αρκετές φορές το κόστος αναβάθμισης συμπεριλαμβάνεται στην αγορά των αδειών χρήσης των μερών που συνιστούν το VPN. Η διαχείριση συνήθως ανατίθεται στον ISP που έχει αναλάβει και την εγκατάσταση του VPN.

Τα πλεονεκτήματα που μπορεί να έχει ένα VPN έχουν καθιερωθεί και έχουν αποδειχθεί. Όμως επειδή τα VPN σχεδιάστηκαν για τα στάσιμα και από σημείο σε σημείο δίκτυα, στερούνται τα χαρακτηριστικά γνωρίσματα κινητικότητας που απαιτούνται για τα σημερινά ασύρματα δίκτυα. Μερικά από τα χαρακτηριστικά γνωρίσματα που λείπουν από τα VPN είναι:

- Δεν υποστηρίζει περιπλάνηση από το ένα δίκτυο στο άλλο (π.χ. από το τοπικό LAN στο υποδίκτυο WI-FI, από WI-FI σε ένα άλλο υποδίκτυο, ή από hot-spot σε 1xRTT).

- Καμία βελτιστοποίηση για τα ασύρματα δίκτυα.

- Καμία αυτόματη ασφάλεια (η επέμβαση χρηστών απαιτείται).

Τα ανωτέρω χαρακτηριστικά που στερείται ένα παραδοσιακό VPN θα μπορούσαν να οδηγήσουν στα ακόλουθα προβλήματα για την επιχείρηση:

- Παραβιάσεις ασφάλειας λόγω του ότι το VPN δεν έχει κάποιο αυτοματοποιημένο μηχανισμό ασφαλείας σε περίπτωση ανάγκης.

- Χαμένη παραγωγικότητα: Όπως έχουμε πει οι χρήστες κινούμενοι σε ένα άλλο δίκτυο είναι αναγκασμένοι να ξανακάνουν αίτησης σύνδεσης. Επίσης πρέπει επανακινούν τις συσκευές κατά τη μετάβαση από το ένα δίκτυο στο άλλο.

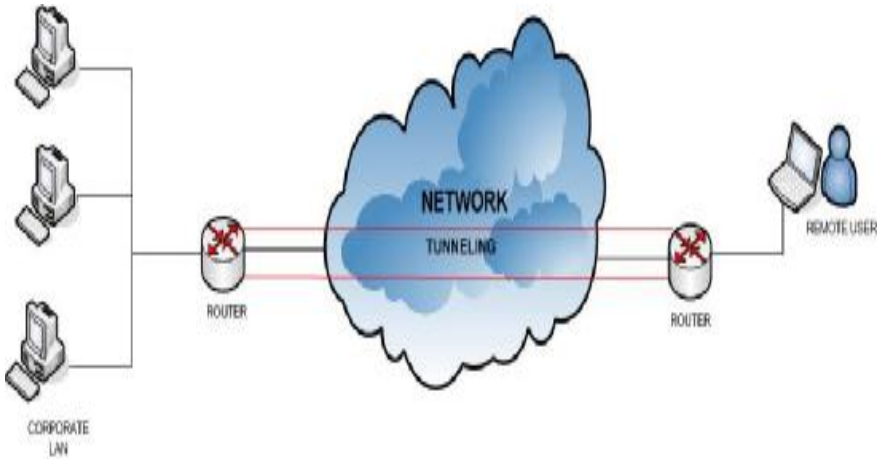
- Αυξανόμενο κόστος υποστήριξης για τους κινητούς χρήστες.

2.5 Κινητά VPN (Mobile VPN)

2.5.1 ΔΙΑΤΥΠΩΣΗ ΠΡΟΒΛΗΜΑΤΟΣ ΚΙΝΗΤΙΚΟΤΗΤΑΣ ΣΤΑ VPN

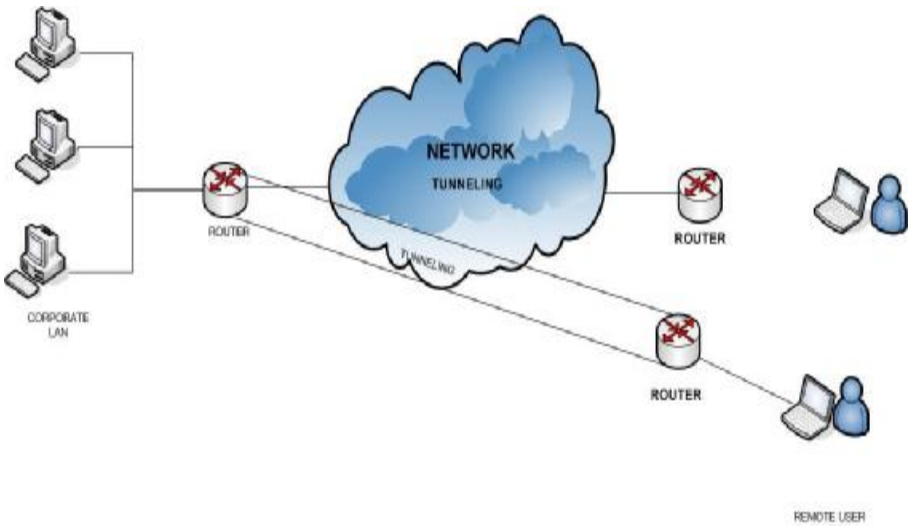
Στα προηγούμενα κεφάλαια είδαμε τα πλεονεκτήματα που μπορεί να έχει ένα δίκτυο VPN. Για παράδειγμα είδαμε πως μπορεί ένα τοπικό εταιρικό δίκτυο να συνδεθεί με ένα άλλο εταιρικό δίκτυο ή με έναν μεμονωμένο χρήστη που βρίσκονται σε μια απομακρυσμένη τοποθεσία. Όμως τι γίνεται στην περίπτωση που έχουμε ένα χρήστη ο οποίος επιθυμεί να έχει πρόσβαση στο δικτυό της εταιρείας του μέσω μιας φορητής συσκευής όπως είναι το laptop, Palmtop,mobilephone κτλ.

Ας υποθέσουμε ότι ο απομακρυσμένος χρήστης βρίσκεται στο ξενοδοχείο και θέλει να μπει από εκεί στο εταιρικό δίκτυο έχοντας ένα φορητό υπολογιστή. Ο υπολογιστής μέσω μιας CPE device συνδέεται με τον τοπικό provider της περιοχής και αποκτά μια συγκεκριμένη IP address που χρησιμεύει ως αναγνωριστικό του υπολογιστή. Στη συνέχεια ο ISP της περιοχής στέλνει ένα μήνυμα στον ISP της περιοχής που βρίσκεται το εταιρικό δίκτυο ότι ο χρήστης με μια διεύθυνση IP επιθυμεί να έχει πρόσβαση στο δίκτυο. Ύστερα από μια ανταλλαγή πακέτων και αφού διαπίστωσει ο ISP ότι ο χρήστης πληρεί τις προδιαγραφές ιδρύεται έναν tunneling μεταξύ του εταιρικού δικτύου και του χρήστη. Έτσι όσα πακέτα ανταλλάζονται μεταξύ αυτών περνάνε μέσα από αυτό το tunneling. Η δρομολόγηση των πακέτων που προέρχονται από το εταιρικό δίκτυο και προορίζονται για τον χρήστη γίνεται με το διάβασμα της IP address(διεύθυνση) που έχει ο καθένας από αυτούς. Όπως είναι λογικό το IP που έχει ο κάθε υπολογιστής που αποτελούν το τοπικό δίκτυο δεν μεταβάλλεται κατά της διάρκειας της σύνδεσης. Ο φορητός υπολογιστής από την στιγμή που έχει πρόσβαση αποκτά μια προσωρινή IP address.



Σχήμα 1. Σύνδεση VPN

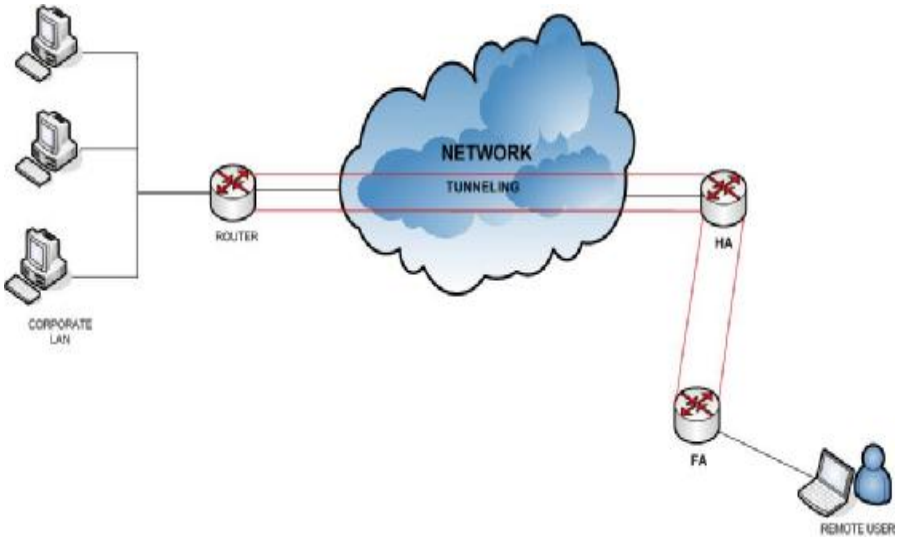
Στη περίπτωση που όμως ο χρήστης αρχίσει να κινείται από την περιοχή που βρίσκεται προς σε μια άλλη περιοχή η σύνδεση αυτή διακόπτεται. Αυτό γίνεται γιατί τα πακέτα που προορίζονται για τον απομακρυσμένο χρήστη συνεχίζονται να έρχονται στο σημείο που βρισκόταν πριν και ο τοπικός πράκτορας που τα παραλάμβανε και τα προωθούσε σε αυτόν δεν ξέρει που να τα στείλει αφού δεν υφίσταται πλεον η IP address του. Έχει κινηθεί σε μια άλλη περιοχή που υπάρχει άλλος ISP οπότε πρέπει να ξανακάνει αίτηση για νέα σύνδεση οπότε θα πρέπει να ιδρυθεί ένα νέο tunneling.



Σχήμα 2. Σύνδεση VPN σε ξένο δίκτυο

2.5.2. ΛΥΣΗ ΣΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΚΙΝΗΤΙΚΟΤΗΤΑΣ

Την λύση στο παραπάνω πρόβλημα μπορεί να μας την δώσει η χρήση του πρωτοκόλλου Mobile IP. Με το Mobile IP ο χρήστης έχει τη δυνατότητα να κρατάει την ίδια IP address κινούμενος σε ένα ξένο δίκτυο. Όταν ο χρήστης βρίσκεται στο δίκτυο από το οποίο συνδέθηκε πρώτη φορά ο τοπικός πράκτορας διαβιβάζει τα πακέτα στον χρήστη. Κινούμενος ο χρήστης προς σε μια άλλη περιοχή τα πακέτα που προορίζονται για αυτόν παραδίδονται στη νέα του θέση αφου ο τοπικός πράκτορας της περιοχής που βρισκόταν προηγουμένως ο χρήστης τα προωθεί σε έναν πράκτορα της περιοχής που βρίσκεται αυτή τη χρονική στιγμή ο χρήστης.



Σχήμα 1. Σύνδεση MVPN

2.5.3 Η ανάγκη ύπαρξης ενός Mobile VPN

Τα κινητά προϊόντα και οι κινητές υπηρεσίες σχεδιάζονται για να αυξήσουν την παραγωγικότητα των κινητών επαγγελματιών. Οι λύσεις εξελίσσονται και πολλαπλασιάζονται και οι εταιρείες βρίσκονται αντιμέτωποι με τις πολυάριθμες προκλήσεις σχετικές με τη διατήρηση της ασφάλειας δικτύων παρέχοντας την απαραίτητη υποστήριξη για τους χρήστες τους. Οι χρήστες πρέπει να είναι σε θέση να έχουν πρόσβαση

στους εταιρικούς πόρους δικτύων ανεξάρτητα από όπου είναι. Εάν είναι στο γραφείο, πρέπει να είναι σε θέση να χρησιμοποιήσουν το ενσύρματο ή ασύρματο τοπικό LAN. Εάν είναι στο δρόμο, πρέπει να πάρουν την πρόσβαση στους ίδιους πόρους χρησιμοποιώντας τα ασύρματα δίκτυα εκτενών ζωνών.

Τη λύση στο παραπάνω πρόβλημα ενδέχεται να λύσουν τα κινητά εικονικά δίκτυα. Είναι βέβαιο ότι τα κινητά εικονικά ιδιωτικά δίκτυα MVPN μπορούν να θεωρούνται τα VPN επόμενης γενιάς που σχεδιάζονται ιδιαίτερα για τις επιχειρήσεις με υπαλλήλους που είναι κινητοί μέσα και έξω από το γραφείο. Συνδυάζουν τα αποδεδειγμένα χαρακτηριστικά γνωρίσματα ασφάλειας που βρίσκονται στα παραδοσιακά VPNs και τις προσωπικές αντιπυρικές ζώνες, με τα χαρακτηριστικά γνωρίσματα κινητικότητας και απλότητας που προσφέρουν τα κινητά μέσα.

Σήμερα οι ασύρματες τεχνολογίες όπως είναι το Wi-Fi, hot spots, 1xRTT βρίσκονται σε συνεχή ανοδική πορεία και εξελίσσονται συνεχώς. Αυτές σε συνδυασμό τη συνεχή χρήση των υπαρχόντων δικτύων όπως το τοπικό LAN, DSL, και τα cable modem οι κάνουν ένα κινητό VPN απαραίτητο για την επιχειρηματική ασφάλεια και κινητικότητα.

Οι διευθυντές θα πρέπει να βεβαιώνονται ότι η ασύρματη εφαρμογή του τοπικού LAN τους είναι ασφαλής και ότι οι συνδέσεις που γίνονται από τις κινητές συσκευές των χρηστών έξω από το γραφείο δεν εκθέτουν το εταιρικό δίκτυο. Με τα MPVN η μετάβαση από το τοπικό LAN στο ασύρματο τοπικό LAN ασφαλή, ανοίγοντας την κρυπτογράφηση αυτόματα όταν χρησιμοποιείται το ασύρματο τοπικό LAN. Στο δρόμο, οι χρήστες μπορούν να συνδέσουν με το εταιρικό δίκτυό τους χρησιμοποιώντας οποιαδήποτε διαθέσιμη σύνδεση, ενσύρματη η ασύρματη. Τέλος, οι χρήστες μπορούν να συνδέθουν από το σπίτι χρησιμοποιώντας την ευρυζωνική σύνδεση της επιλογής τους.

2.5.4. Πλεονεκτήματα ενός Mobile VPN

● Οι χρήστες δεν χρειάζεται να ξεκινήσουν μια νεα session και έτσι μπορούν να κινηθούν από το ένα δίκτυο

στο άλλο χωρίς την απώλεια των δεδομένων τους εξαιτίας επανεκκίνηση των εφαρμογών τους και συσκευών τους.
● Αυτοματοποιημένοι μηχανισμοί ασφαλείας όπως καθορίζονται από τις πολιτικές της εταιρίας χωρίς να την επέμβαση του χρήστη.

● Αυτόματη επιλογή του καλύτερου διαθέσιμου δικτύου.

● Επιβάλλει την προστασία συσκευών και δικτύων για να αποφύγει πάντα τις παραβιάσεις ασφάλειας ενώ ο χρήστης είναι κινητός.

● Επιτρέπει τη βελτιστοποίηση για τα ασύρματα δίκτυα, συμπεριλαμβανομένης της συμπίεσης.

√ **Συνεπώς με τα MVPN έχουμε :**

-Αυξανόμενη παραγωγικότητα: Η παραγωγικότητα των κινητών επαγγελματιών αυξάνεται δραματικά λόγω της συνόδου και της ασφαλούς συνδετικότητας. Τα μέλη των κινητών ομάδων εργασίας μπορούν να συνεργαστούν αποτελεσματικά, και οι ανώτεροι υπάλληλοι μπορούν να μείνουν συνδεμένοι με τους εταιρικούς πόρους εύκολα και στον πραγματικό χρόνο χρησιμοποιώντας τις υπάρχουσες αιτήσεις των γραφείων τους.

-Χαμηλότερο κόστος υποστήριξης: Με τα MVPN, οι χρήστες συνδέονται με την επιχείρηση αυτόματα χρησιμοποιώντας το καλύτερο διαθέσιμο δίκτυο χωρίς οποιαδήποτε επέμβαση.

-Ενισχυμένη ασφάλεια: Το MVPN επικαλείται την ασφάλεια αυτόματα και επιβάλλει τις πολιτικές ασφάλειας της επιχείρησης που αποτρέπει τους χρήστες από την παραγωγή των λαθών που θα μπορούσαν να εκθέσουν τη συσκευή του χρήστη καθώς επίσης και το επιχειρηματικό δίκτυο.

3. ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Στο παραπάνω κεφαλαίο αναλύσαμε τι είναι ένα δίκτυο vpn(εικονικό ιδιωτικό δίκτυο),πως μπορεί να υλοποιηθεί, το ρόλο που παίζει σε μια επιχείρηση καθώς τα πλεονεκτήματα και τα μειονεκτήματά τους. Στο επόμενο κεφάλαιο θα αναφερθούμε πως μπορεί να προστατευτεί το δίκτυο αυτό από διάφορες επιθέσεις όπως επίσης να το κάνουμε ασφαλέστερο και πιο αξιόπιστο.

ΜΕΡΟΣ 3ο

1. ΑΣΦΑΛΕΙΑ VPN

1.1 Κρυπτογραφία(encryption)

Ένα από τα κυριότερα θέματα για τα VPN είναι η ασφαλής μετάδοση των δεδομένων χωρίς να παρέχεται η δυνατότητα σε τρίτους να υποκλέψουν τα δεδομένα της επικοινωνίας. Έτσι πρέπει να γίνουν κάποια βήματα προς την μεριά της ασφάλειας των δεδομένων. Όπως θα δούμε παρακάτω υπάρχει μια ευρεία γκάμα αλγορίθμων κρυπτογράφησης σχεδόν για όλα τα επίπεδα του OSI και αυτό που απομένει στον χρήστη του VPN είναι να διαλέξει το επίπεδο ασφαλείας που επιθυμεί σύμφωνα με τις εφαρμογές που χρησιμοποιεί. Παρακάτω θα κάνουμε μια εισαγωγή στους κυριότερους κρυπτογραφικούς αλγορίθμους για να πάρουμε μια πρώτη ιδέα του θεωρητικού υπόβαθρου τους. Στο επόμενο κεφάλαιο θα δούμε πώς χρησιμοποιούνται αυτοί οι κρυπτογραφικοί αλγόριθμοι σε συνεργασία με άλλα VPN πρωτόκολλα για να ενισχύσουν την ασφάλεια των VPN δικτύων.

Η ασφάλεια των VPN βασίζεται στην κρυπτογραφική δυνατότητα των αλγορίθμων κρυπτογράφησης. Θεωρούμε ότι είναι ανάγκη να παρουσιασθούν ορισμένα βασικά στοιχεία των διαφόρων αλγορίθμων ούτως ώστε να μπορούμε να δούμε το θέμα της ασφάλειας των VPN και από μία πιο σφαιρική εικόνα.
Μία κρυπτογραφική διαδικασία είναι η μετατροπή ενός απλού κειμένου σε ένα κρυπτογραφημένο κείμενο όπως για παράδειγμα η πρόταση: “Η ασφάλεια στα VPN είναι ζωτικής σημασίας” στην κρυπτογραφημένη πρόταση “ςεθ235φ5345η55θ67ε5ηφ675ςε78ηηβ6”.
Αποκρυπτογράφηση είναι η ακριβώς αντίθετη διαδικασία, δηλαδή η μετατροπή της κρυπτογραφημένης πρότασης “ςεθ235φ5345η55θ67ε5ηφ675ςε78ηηβ6” στην μη κρυπτογραφημένη πρόταση “Η ασφάλεια στα VPN είναι ζωτικής σημασίας”. Όπως έχουμε δει τα δυο κείμενα (απλό, κρυπτογραφημένο) δεν φαίνονται να έχουν κάποια σχέση μεταξύ τους. Το κρυπτογραφημένο φαίνεται εκ πρώτης όψεως ότι είναι σκουπίδια. Αυτά τα δύο κείμενα τα συνδέει μεταξύ τους μια συνάρτηση f(x) η οποία είναι το κλειδί της κρυπτογράφησης.

Ένα άλλο μεγάλο θέμα για τα VPN είναι αν ένας κρυπτογραφικός αλγόριθμος μπορεί να « σπάσει », αν δηλαδή τα δεδομένα του είναι ασφαλή από την επίδραση τρίτων και αν ο αποστολέας είναι πραγματικά αυτός που ισχυρίζεται ότι είναι. Παρακάτω θα δούμε διάφορους αλγορίθμους οι οποίοι μπορούν να το κάνουν αυτό.

1.2. Ιδιωτικό Κλειδί (Private Key)

Σε αυτόν τον αλγόριθμο ο αποστολέας και ο παραλήπτης ενός κειμένου χρησιμοποιούν το ίδιο κλειδί το οποίο μόνο αυτοί οι δύο γνωρίζουν (private κλειδί). Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το κείμενο και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να το αποκρυπτογραφήσει. Αυτή η μέθοδος κρυπτογραφίας ονομάζεται μυστικού κλειδιού (secret key) ή συμμετρική κρυπτογραφία και θεωρείται μία από τις πιο ασφαλείς μεθόδους. Όμως ένα σοβαρό πρόβλημα της μεθόδου αυτής είναι με πιο τρόπο ο αποστολέας και ο παραλήπτης θα συμφωνήσουν για το κλειδί, και πώς θα το ανταλλάξουν μεταξύ τους. Το πρόβλημα γίνεται πιο οξύ όταν ο αποστολέας και ο παραλήπτης βρίσκονται σε διαφορετική γεωγραφική περιοχή. Σε αυτή την περίπτωση τίθεται ένα πιο γενικό θέμα, αν μπορούν να εμπιστευτούν είτε το δίκτυο, είτε το ταχυδρομείο είτε το τηλέφωνο. Αν και αυτή η μέθοδος θεωρείται αρκετά ασφαλής είναι δύσκολο να εφαρμοσθεί σε δίκτυα VPN όπου οι διάφοροι hosts δε βρίσκονται στην ίδια γεωγραφική περιοχή. Αν λάβουμε υπόψη ότι τα περισσότερα δίκτυα VPN συνδέουν υπολογιστές που βρίσκονται σε πολύ μακρινές αποστάσεις (διαφορετικές γεωγραφικές περιοχές) μπορούμε να θεωρήσουμε ότι σπάνια χρησιμοποιείται και σε πολύ εξειδικευμένες περιπτώσεις π.χ. στρατιωτικές εφαρμογές ή σε δίκτυα VPN που χρησιμοποιούνται σε κλειστά τραπεζικά συστήματα όπου ο διαχειριστής όλων των κλειδιών είναι ένας και μοναδικός.

1.3. Δημόσιο Κλειδί (Public Key)

Οι Whitfield Diffie και Martin Hellman το 1976 παρουσίασαν την κρυπτογραφική μέθοδο δημόσιου κλειδίου (public key) που σκοπό είχε να λύσει το πρόβλημα που παρουσιαζόταν στην μετάδοση του κλειδιού της μεθόδου private key. Σε αυτήν την μέθοδο ο αποστολέας και ο παραλήπτης έχουν από ένα public και ένα private κλειδί. Το public κλειδί είναι σε όλους γνωστό (μπορεί να βρεθεί σε διάφορα ευρετήρια), ενώ το private κλειδί το γνωρίζει μόνο ο κάτοχός του. Σε αυτό το είδος κρυπτογράφησης δεν είναι ανάγκη τα κανάλια να είναι ασφαλή γιατί ουσιαστικά μόνο ο κατάλληλος παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και άρα να το δει.

Τα πλεονεκτήματα της χρήσης public κλειδιού είναι η ασφάλεια και η ευκολία που παρέχεται σε αντίθεση με το private κλειδί το οποίο δεν είναι σωστό να μεταδίδεται μέσω του δικτύου ή να δίδεται σε άλλο τρίτο άτομο. Ένα άλλο πλεονέκτημα του public κλειδιού είναι η δυνατότητα παροχής αξιόπιστων ηλεκτρονικών υπογραφών.

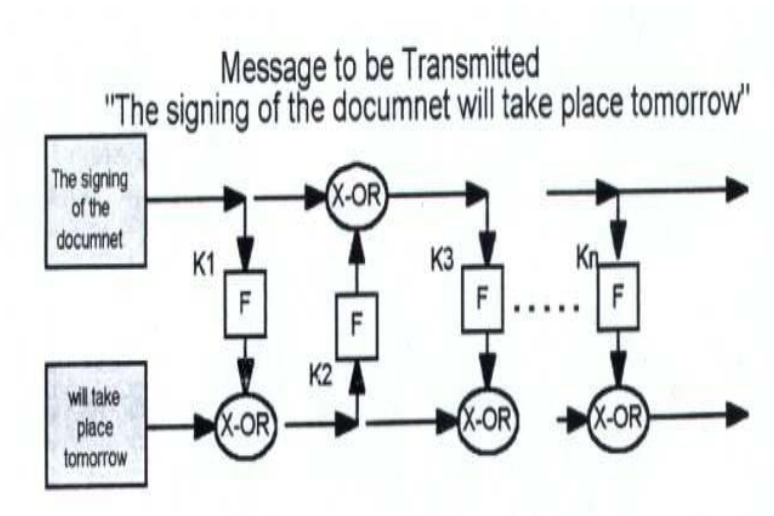
Ένα σοβαρό μειονέκτημα των public key αλγορίθμων είναι η πολύ μικρή ταχύτητα τους ενώ αντίθετα οι private key αλγόριθμοι είναι σημαντικά γρηγορότεροι. Έτσι εκμεταλλευόμενοι τα πλεονεκτήματα των δύο πιο πάνω κρυπτογραφικών αλγορίθμων έχουμε δημιουργήσει διάφορες “digital envelope” μεθόδους οι οποίες συνδυάζουν τις δύο ανωτέρω μεθόδους και συμπεριφέρονται πάρα πολύ καλά.

1.4. Block Ciphers

Block Cipher είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος επαναλαμβάνει διάφορες λειτουργίες όπως αντικατάσταση, μετάθεση, πολλαπλασιασμό, και γραμμικούς μετασχηματισμούς δημιουργώντας έτσι ένα πολύ πιο δυνατό αλγόριθμο. Η αποκρυπτογράφηση αυτής της μεθόδου γίνεται με τον αντίστροφο αλγόριθμο της κρυπτογράφησης.

1.5. Data Encryption Standards - DES

Ο Data Encryption Standards έχει αναπτυχθεί στην IBM και είχε αρχικά ονομασθεί Lucifer. Ο DES είναι ένας αλγόριθμος ο οποίος χρησιμοποιεί 64-bit μέγεθος block και ένα κλειδί 56-bit.



Σχήμα 1. Feistel cipher

Γενικά ο αλγόριθμος αυτός δεν είναι εύκολο να δεχθεί επιθέσεις, αλλά υπάρχει ένας μηχανισμός ο οποίος μπορεί να τον σπάσει. Ένας τέτοιος μηχανισμός είναι η "brute-force attack"(επίθεση μαζικής δύναμης), η οποία προσπαθεί να βρει όλους τους δυνατούς συνδυασμούς που μπορούν να γίνουν και άρα να βρει και τον σωστό συνδυασμό. Μια άλλη τεχνική ονομάζεται "sustained data analysis"(υποστηρικτική ανάλυση δεδομένων) , την οποία βλέπουμε στη παρακάτω εικόνα:

Wfhrhewpfwe fhwefh 8eemgwergwe7n13-8-132jgk4kh2lj8@-76&1
Bkjlsdf09f-893r;1 ;l1m= fljm=9*|++eemM832[0
&)0-7-31mfdeemmqp8j03mdasx
unfw2y067109760)asdsa(&^%eemaca$$gxoasg
7@#7^ypoeemiuw2-wefwef3wee-kin
0f9qbeemupouthf30-53^&^))Peem6p4c23

Εδώ βλέπουμε τρία κρυπτογραφημένα μηνύματα τα οποία έχουν κρυπτογραφηθεί με το ίδιο κλειδί, αν παρατηρούμε λιγάκι προσεκτικά βλέπουμε ότι και στα τρία κρυπτογραφημένα μηνύματα υπάρχουν ορισμένοι

χαρακτήρες που είναι με την ίδια σειρά και άρα έχουν προέλθει από το ίδιο κλειδί. Αν αυτοί οι χαρακτήρες έχουν μεγάλη συχνότητα εμφάνισης τότε κάποιος μπορεί να συμπεράνει με μεγάλη πιθανότατα ποια είναι αυτή η λέξη. Αυτή η λέξη μπορεί να αντιστοιχεί σε μια λέξη που παρουσιάζει μεγάλη συχνότητα εμφάνισης όπως για παράδειγμα η λέξη “και”. Με αυτό τον τρόπο μπορεί κανείς να σπάσει το DES. Η λύση σε αυτό το πρόβλημα είναι βεβαίως η συχνή αλλαγή των κλειδιών.

1.6 Hash Functions (Συναρτήσεις Κατακερματισμού)

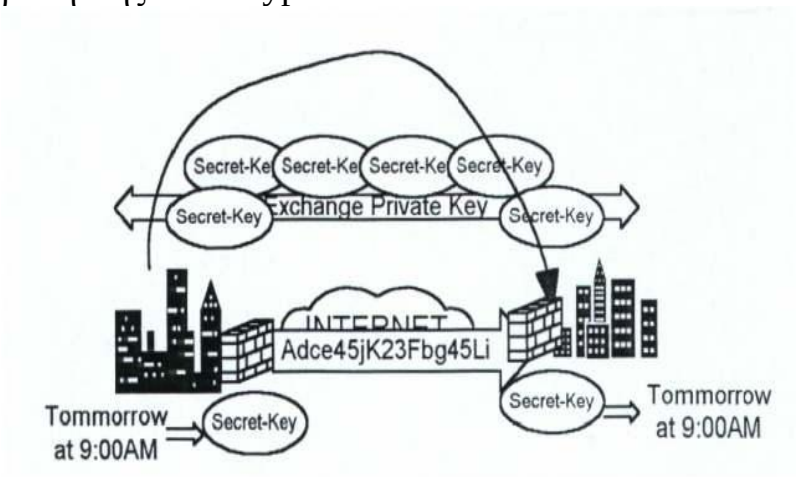
Οι hash συναρτήσεις, είναι συναρτήσεις οι οποίες παίρνουν ένα μεταβλητού μεγέθους μήνυμα και μας δίνουν ένα fixed length(διορθωμένο μήκους) μήνυμα, συνήθως 128 bit ή περισσότερα, το οποίο αναφέρεται σαν hash τιμή. Οι hash συναρτήσεις είναι μονόδρομες (one way) δηλαδή είναι πολύ δύσκολο να βρεθεί η αντίστροφη συνάρτηση τους και άρα να σπάσουν. Δηλαδή αν δοθεί ένα μήνυμα και μια hash συνάρτηση και δημιουργηθεί μια hash τιμή θα πρέπει να είναι αδύνατη η αναπαραγωγή του κλειδιού από την hash τιμή. Όταν σε ένα έγγραφο εφαρμοσθεί η hash συνάρτηση το αποτέλεσμα είναι ένα δακτυλικό αποτύπωμα του αρχικού εγγράφου. Έτσι αυτή η μέθοδος χρησιμοποιείται ευρέως σε ηλεκτρονικές υπογραφές. Υπάρχουν αρκετές υλοποιήσεις των hash συναρτήσεων όπως για παράδειγμα τα Message Digest 2,4,5 (MD2), (MD4), (MD5), ο Secure hash αλγόριθμος (SHA και SHA-1).

2. Εφαρμογές κρυπτογραφίας

Στην προηγούμενη ενότητα, έγινε μια εισαγωγή στις έννοιες της κρυπτογραφίας και στις διάφορες υλοποιήσεις που έχουν αναπτυχθεί μέχρι σήμερα. Η κρυπτογραφία αποτελεί μια διαδικασία επίλυσης δύσκολων προβλημάτων. Σε αυτή την ενότητα θα μελετηθεί το πως αυτή εφαρμόζεται στα VPNs, στα διάφορα πρότυπα των VPNs, όπως και στα διάφορα πρωτόκολλα που χρησιμοποιούνται.

2.1. Κρυπτογράφηση Ιδιωτικού Κλειδιού(Private key encryption)

Το private key encryption βασίζεται στη λογική του private key όπου το ίδιο κλειδί κωδικοποιεί και αποκωδικοποιεί το μήνυμα. Όπως έχουμε ήδη αναφέρει αν και αυτή η μέθοδος είναι πάρα πολύ καλή, το μεγαλύτερο πρόβλημα της είναι το πώς θα παραλάβει ο παραλήπτης το encryption κλειδί.



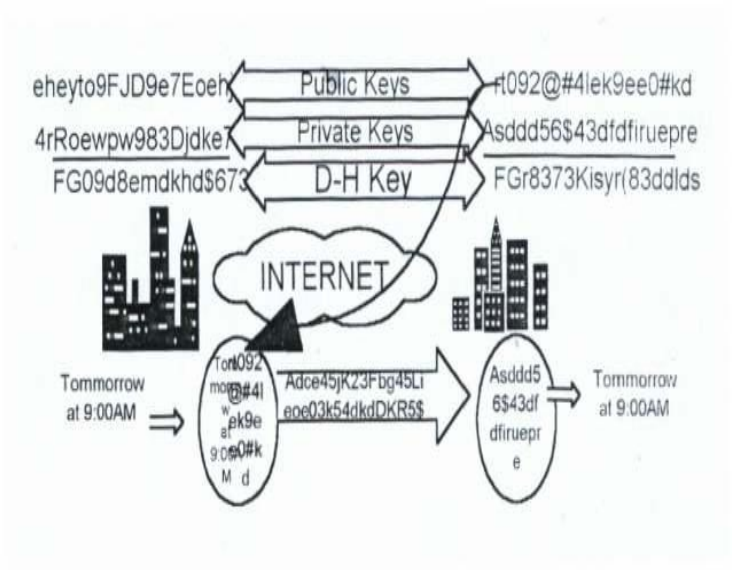
Σχήμα 1. Διαδικασία private encryption

Στο παραπάνω σχήμα (1) παρατηρούμε με ποιο τρόπο κωδικοποιείται, μεταφέρεται και αποκωδικοποιείται το κρυπτογραφημένο μήνυμα αλλά και πως γίνεται η ανταλλαγή του secret key(μυστικό κλειδί). Παρατηρούμε ότι το secret key για μεγαλύτερη ασφάλεια δεν μεταφέρεται με το ίδιο μέσο με το οποίο μεταφέρεται και το κωδικοποιημένο μήνυμα.
Εκτός αυτού του σοβαρού μειονεκτήματος, σε τέτοιου

είδους συστήματα ο αριθμός των κλειδιών είναι υπερβολικά μεγάλος γιατί κάθε ζεύγος χρηστών πρέπει να έχει και από ένα κλειδί. Όσο περισσότερα κλειδιά χρειάζονται, τόσο η διαχείριση και η διανομή των κλειδιών γίνεται δυσκολότερη. Για παράδειγμα, αν ένας οργανισμός έχει 100 χρήστες VPN τότε απαιτούνται 4950 κλειδιά (100*99/2), τι γίνεται στην περίπτωση που ένας οργανισμός έχει 1000 χρήστες (συνηθισμένη περίπτωση), τότε απαιτείται το εξωπραγματικό νούμερο των 499,500 κλειδιών. Άρα παρατηρούμε ότι είναι αδύνατο αυτή η μέθοδος να υλοποιηθεί σε πραγματικά εμπορικά VPN.

2.2.Κρυπτογράφηση Δημόσιου Κλειδιού(Public key encryption)

Στο public key encryption όπως έχουμε αναφέρει στην προηγούμενη ενότητα απαιτούνται δύο κλειδιά, ένα private το οποίο είναι γνωστό μόνο στο χρήστη του και σε κανένα άλλο και ένα public το οποίο είναι διαθέσιμο στον καθένα και μπορεί να βρεθεί σε διάφορα ευρετήρια. Το private key που αναφέρουμε εδώ δεν σχετίζεται με το private key που αναφέρεται στην προηγούμενη παράγραφο (μέθοδος private κλειδιού), αλλά αυτό το private key απλά αποκρυπτογραφεί μηνύματα τα οποία έχουν κρυπτογραφηθεί με το σχετικό public key.

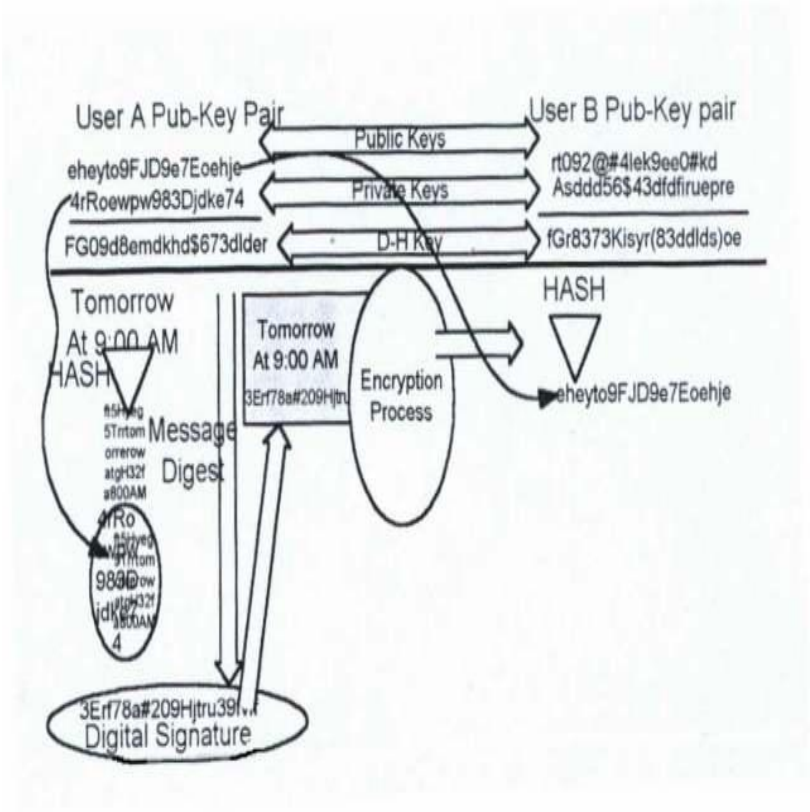


Σχήμα 2. Public Key Encryption

Δύο πολύ γνωστά public key συστήματα που χρησιμοποιούνται σήμερα στα VPN είναι το Rivest Shamir Adlemen (RSA) και το Diffie- Hellman (DH). Στην πιο πάνω εικόνα παρατηρούμε ένα encryption σχήμα που χρησιμοποιεί το DH σύστημα που έχουμε αναφέρει. Ο αποστολέας μπορεί να πάρει το public key του παραλήπτη από διάφορες πηγές, στη συνέχεια κωδικοποιεί το μήνυμα “Tomorrow at 9:00 am” χρησιμοποιώντας αυτό το public key. Ακολούθως, το κρυπτογραφημένο μήνυμα στέλνεται στον παραλήπτη μέσω ενός δημόσιου δικτύου. Ο παραλήπτης λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το private key του. Όμως όπως έχει αναφερθεί αυτή η μέθοδος είναι πολύ αργή και έτσι χρησιμοποιείται ένας συνδυασμός των δύο πιο πάνω μεθόδων, δηλαδή του private key encryption και public key encryption ο οποίος βελτιώνει κατά πολύ την κατάσταση χρησιμοποιώντας τα πλεονεκτήματα της κάθε μεθόδου. Δηλαδή, η επικοινωνία των κωδικοποιημένων μηνυμάτων θα γίνεται με private key encryption, αφού είναι πολύ πιο γρήγορη η αποκρυπτογράφηση, αλλά η αρχική μεταφορά του μηνύματος και του private key θα γίνεται με public key encryption και άρα λύνεται το πρόβλημα της αξιόπιστης μεταφοράς του κλειδιού.

2.3. Ψηφιακές Υπογραφές(Digital Signatures)

Για να αυξηθεί η αξιοπιστία των VPN, οι χρήστες τους μπορούν να χρησιμοποιούν ψηφιακές υπογραφές και με αυτόν τον τρόπο να ελέγχουν την πιστότητα των δεδομένων αλλά και των προσώπων που βρίσκονται στο άλλο άκρο. Οι ψηφιακές υπογραφές είναι ένα είδος κρυπτογράφησης το οποίο χρησιμοποιεί hash συναρτήσεις. Στο Σχήμα 3(επόμενη σελίδα) βλέπουμε την διαδικασία δημιουργίας μιας ψηφιακής υπογραφής.



Σχήμα 3. Διαδικασία Digital Signatures

Παρατηρούμε ότι ο χρήστης Α περνάει το μήνυμα από μια hash συνάρτηση, μετά το μειώνει στα 128-bits και το κρυπτογραφεί με το private key του. Μέχρι εδώ ο χρήστης Α έχει δημιουργήσει την ψηφιακή του υπογραφή. Τώρα η υπογραφή του μαζί με το αρχικό μήνυμα κρυπτογραφούνται ξανά και στέλνονται στον παραλήπτη. Ο παραλήπτης τότε κάνει τις εξής δύο λειτουργίες: πρώτα αποκρυπτογραφεί το αρχικό μήνυμα και ακολούθως την υπογραφή του αποστολέα και τα συγκρίνει και έτσι μπορεί να γνωρίζει αν πράγματι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται ότι είναι και ότι το μήνυμα στάλθηκε από το σωστό άτομο.

2.4. RSA Public-Key Αλγόριθμος

Το RSA είναι ένα ευρέως γνωστό σύστημα και χρησιμοποιείται πάρα πολύ στα VPN δίκτυα όπως και σε πολλές άλλες εφαρμογές στο Internet. Βασίζεται σε δύο μαθηματικές φόρμουλες: την encryption συνάρτηση, η οποία είναι CT=PTPub mod N, και την decryption συνάρτηση CT=CTPriv mod N, όπου PT είναι το κείμενο, CT το κρυπτογραφημένο κείμενο, Pub το public key, και Priv το private key.

Τα βήματα του RSA υπολογισμού είναι:

I. Πάρε δύο μεγάλους πρώτους αριθμούς, έστω P1 και P2, και πολλαπλασίασε τους, βρες το γινόμενο τους. Το γινόμενο το ονομάζουμε M.

II. Ακολούθως επιλέγουμε ένα αριθμό, τον Pub, ο οποίος είναι μικρότερος από το M, αλλά σχετικά πρώτος στους (P1-1) (P2-1).

III. Βρες ακόμη ένα αριθμό, τον Priv, με τον περιορισμό ότι (PubPriv-1) είναι διαιρετέος από το (P1-1) (P2-1).

IV. Priv είναι ο private εκθέτης του private κλειδιού (M, Priv) και Pub είναι ο public εκθέτης του public κλειδιού (m, Pub).

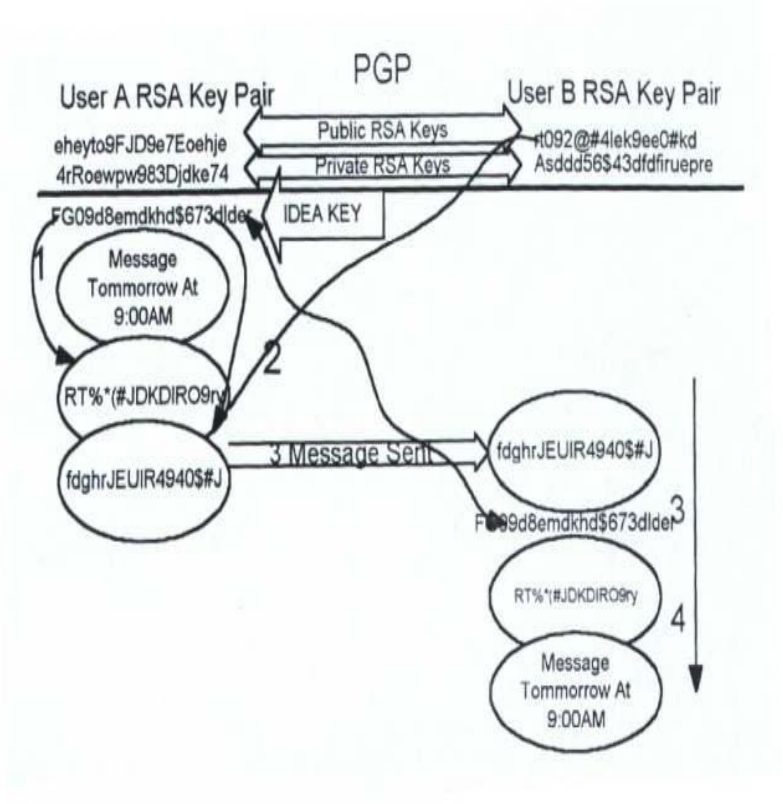
V. Οι δύο μεγάλοι πρώτοι δεν χρειάζονται πλέον και μπορούν να καταστραφούν.

Ο RSA, όπως θα δούμε παρακάτω, χρησιμοποιείται μαζί με τα κατεξοχήν πρωτόκολλα του VPN, τα IPSec και PPTP, για να προσφέρει κρυπτογράφηση.

2.5. Pretty Good Privacy (PGP) (αρκετά καλή ιδιωτικότητα)

Το PGP χρησιμοποιείται σήμερα ευρέως όχι μόνο από χρήστες των VPN δικτύων αλλά και από κάθε είδους χρήστη σε αρκετές εφαρμοφές όπως π.χ το ηλεκτρονικό ταχυδρομείο. Είναι ένα υβριδικό κρυπτοσύστημα, καθώς συνδυάζει τον public key αλγόριθμο και τον private key αλγόριθμο. Το PGP λειτουργεί όπως όλα τα υπόλοιπα public key κρυπτοσυστήματα χρησιμοποιώντας τον RSA public key αλγόριθμο και τον IDEA για encryption. Ένα IDEA κλειδί χρησιμοποιείται για κρυπτογράφηση αλλά και για αποκρυπτογράφηση του μηνύματος και ο RSA χρησιμοποιείται για να κρυπτογραφήσει το IDEA κλειδί μαζί με το public key του παραλήπτη. Ο παραλήπτης,

χρησιμοποιεί το δικό του private κλειδί για να αποκρυπτογραφήσει το κατά RSA κρυπτογραφημένο μήνυμα που έχει λάβει. Χρησιμοποιώντας το αποκρυπτογραφημένο IDEA κλειδί, το οποίο προέκυψε από την αποκρυπτογράφηση του RSA μηνύματος, μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Παρατηρούμε ότι με αυτό τον τρόπο έχουμε ένα απλό, ασφαλή και γρήγορο τρόπο να κρυπτογραφούμε μηνύματα και να τα στέλνουμε με ασφάλεια γνωρίζοντας ότι ο παραλήπτης θα το λάβει και θα το διαβάσει χωρίς κανένα πρόβλημα υποκλοπής.



Σχήμα 4. Επικοινωνία PGP

Στο πιο πάνω σχήμα (4) παρατηρούμε μία PGP επικοινωνία μεταξύ των χρηστών Α και Β. Ο χρήστης Α θέλοντας να στείλει το μήνυμα “Tomorrow at 9:00 a.m.” ακολουθεί μία διαδικασία η οποία περιλαμβάνει τα ακόλουθα βήματα :

→ Ο χρήστης Α κρυπτογραφεί το μήνυμα με το IDEA encryption key.

→ Ο χρήστης Α κωδικοποιεί το IDEA key χρησιμοποιώντας το public key του Β.

→ Το μήνυμα αποστέλλεται στον παραλήπτη που στην προκειμένη περίπτωση είναι ο Β.

→ Ο χρήστης Β χρησιμοποιεί το δικό του RSA private key για να αποκρυπτογραφήσει το κρυπτογραφημένο IDEA κλειδί.
→ Ο χρήστης Β αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το IDEA κλειδί.

2.6. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ - FIREWALLS

Γενικά με τον όρο firewall εννοούμε ένα τμήμα ή σύνολο τμημάτων που περιορίζουν την πρόσβαση μεταξύ ενός προστατευμένου δικτύου και του Internet ή μεταξύ απλά διαφορετικών δικτύων. Τα τμήματα αυτά μπορεί να είναι είτε εσωτερικοί και εξωτερικοί δρομολογητές (interior / exterior routers), είτε ένα υπολογιστικό σύστημα το οποίο είναι το κεντρικό σημείο επαφής μεταξύ των χρηστών του εσωτερικού δικτύου και του Internet (Bastion Host), είτε ένας υπολογιστής που έχει τουλάχιστον δύο κάρτες δικτύου (Dual-homed host), είτε ένα πρόγραμμα που λειτουργεί ως μεσολαβητής μεταξύ των εξωτερικών servers και εσωτερικών clients (Proxy Server).
Παρακάτω περιγράφονται κάποιες έννοιες οι οποίες χρησιμοποιούνται εκτενώς στη συνέχεια:

Host:
Ένα υπολογιστικό σύστημα που βρίσκεται σε ένα δίκτυο.

Dual-Homed Host:
Ένα υπολογιστικό σύστημα με δύο τουλάχιστον κάρτες δικτύου.

Bastion Host:
Ένα υπολογιστικό σύστημα το οποίο θα πρέπει να προφυλαχθεί ιδιαιτέρως επειδή συνήθως εκτίθεται στο internet και αποτελεί το κύριο σημείο επαφής για τους χρήστες των εσωτερικών δικτύων.

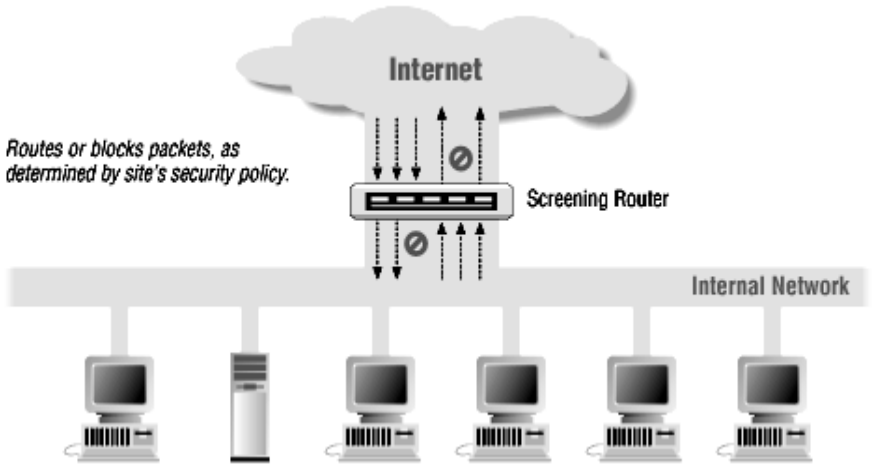
2.7. ΤΕΧΝΟΛΟΓΙΕΣ

Στη συνέχεια περιγράφονται αναλυτικά οι κυριότερες τεχνολογίες που σχετίζονται με firewalls καθώς επίσης και τα πλεονεκτήματα και μειονεκτήματα που έχει κάθε τεχνολογία ξεχωριστά. Αυτές είναι οι εξής:

- Packet filtering
- Proxy services
- Network Address Translation

2.7.1. Packet Filtrering

Τα συστήματα που εκτελούν το φιλτράρισμα πακέτων, ανάλογα με τη πολιτική που ακολουθείται σε κάθε site, επιτρέπουν ή μπλοκάρουν την κίνηση συγκεκριμένων πακέτων μεταξύ μηχανημάτων που ανήκουν σε διαφορετικά δίκτυα. Ο τύπος του δρομολογητή που χρησιμοποιείται για το φιλτράρισμα των πακέτων ονομάζεται screening router.



Σχήμα 1. Χρησιμοποίηση screening router για φιλτράρισμα πακέτων

√ Τρόποι διαμόρφωσης packet filtering:

• Packet Filtering in Routers

Ένας δρομολόγητής έχει τη δυνατότητα να συλλέξει ακόμα και πληροφορίες σχετικά με τα δεδομένα των πακέτων πέρα από αυτές που του παρέχονται από τους headers, και να ελέγξει αν πράγματι είναι τα προσδοκώμενα για κάποια συγκεκριμένη πόρτα. Η ικανότητα αυτή βοηθά στην ανακάλυψη των γνωστών DoS επιθέσεων που βασίζονται στην αποστολή μεταλλαγμένων πακέτων.
Επίσης ένας δρομολογητής γνωρίζει πληροφορίες όπως:

- Το interface στο οποίο πρόκειται να φθάσει το πακέτο
- Το interface από το οποίο θα φύγει το πακέτο

Τέλος, ο δρομολογητής που παρακολουθεί την κίνηση των πακέτων γνωρίζει κάποια επιπλέον πράγματα όπως:
1. Τον πρόσφατο αριθμό των πακέτων που έχουν σταλεί ή ληφθεί από το ίδιο host,
2. Εάν το τρέχων πακέτο είναι πανομοιότυπο ή όχι με κάποιο πρόσφατο πακέτο,
3. Εάν το πακέτο αυτό αποτελεί μέρος μεγαλύτερου πακέτου.

Έτσι ένας απλός δρομολογητής έχει τη δυνατότητα να δρομολογεί πακέτα εξετάζοντας μόνο τη διεύθυνση προορισμού τους. Σε αντίθεση με αυτόν, ο screening router πέρα από το να ελέγξει αν υπάρχει η δυνατότητα δρομολόγησης του πακέτου με βάση την διεύθυνση προορισμού, ελέγχει και αν θα έπρεπε να προχωρήσει στην δρομολόγηση. Κατανοώντας τις λειτουργίες και τις διαφορές μεταξύ των δρομολογητών βλέπουμε ότι ο screening router έχει τη δυνατότητα να κάνει ένα από τα παρακάτω:
- Να στείλει τελικά το πακέτο στον προορισμό του,
- Να απορρίψει το πακέτο χωρίς να κάνει καμία ενημέρωση στον αποστολέα,
- Να αρνηθεί να προωθήσει το πακέτο επιστρέφοντας κάποιο μήνυμα λάθους στον αποστολέα,
- Να συλλέξει πληροφορίες για το πακέτο,

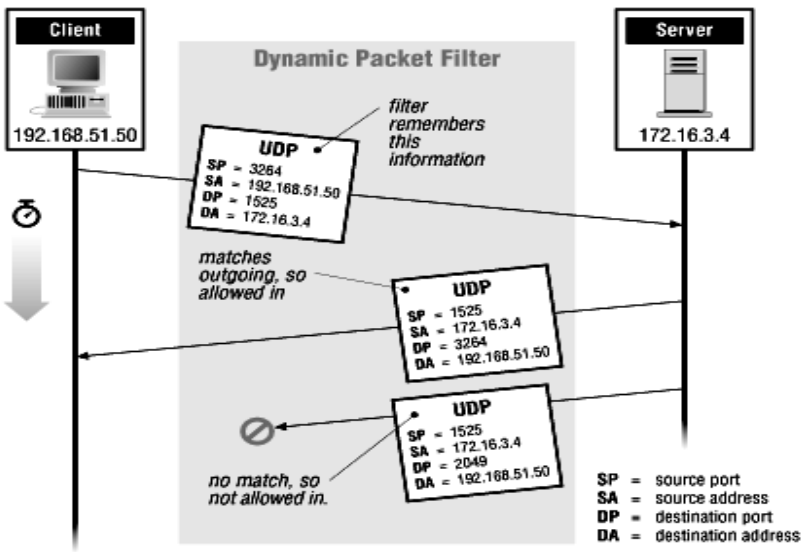
- Να στείλει κάποια προειδοποίηση (alarm)

Ακόμα κάποιοι περισσότερο “έξυπνοι” δρομολογητές είναι ικανοί να κάνουν τα εξής:
- Να τροποποιήσουν το πακέτο (αλλαγή διεύθυνσης προέλευσης μέσω NAT)
- Να στείλουν το πακέτο σε άλλη διεύθυνση από αυτή που προοριζόταν (να το στείλουν σε κάποιον proxy server)
- Να τροποποιήσουν τους κανόνες φιλτραρίσματος (να αρνηθούν κάθε είδους κίνηση από κάποιο site που έχει στείλει «εχθρικό» πακέτο)

• Stateful packet filtering

Οι δρομολογητές που εκτελούν το φιλτράρισμα των πακέτων δεν έχουν όλοι τις ίδιες ικανότητες. Το φιλτράρισμα που γίνεται από συστήματα που έχουν την ικανότητα να διατηρούν λεπτομέρειες για την κατάσταση της συναλλαγής λέγεται stateful packet filtering ή dynamic packet filtering επειδή η συμπεριφορά του συστήματος αλλάζει ανάλογα με την κίνηση που παρακολουθεί.

Στο παρακάτω σχήμα φαίνεται ένα παράδειγμα δυναμικού φιλτραρίσματος πακέτου όπου το δεύτερο εισερχόμενο UDP πακέτο απορρίπτεται.



Σχήμα 2. Δυναμικό φιλτράρισμα πακέτου στην UDP Layer

Συνοψίζοντας τους κανόνες για το φιλτράρισμα πακέτων, υπάρχουν πολλοί διαφορετικοί τρόποι καθορισμού των φίλτρων σε έναν δρομολογητή. Κάποιοι δομολογητές απαιτούν ένα γενικό κανόνα που εφαρμόζεται σε όλα τα υπό δρομολόγηση πακέτα και κάποιοι άλλοι απατούν ρυθμίσεις σε κάθε interface ξεχωριστά.

• IPchains

Το φιλτράρισμα πακέτων σε συστήματα LINUX γίνεται με τη βοήθεια του συστήματος ipchains που συμπεριλαμβάνεται στον πυρήνα του λειτουργικού.

Η ιδέα του συστήματος είναι η εξής: υπάρχει μια αλυσίδα από κανόνες και ένας στόχος για κάθε κανόνα. Έτσι κάθε πακέτο για κάθε κανόνα που ικανοποιεί θα υποστεί τις ανάλογες ρυθμίσεις για την ικανοποίηση του στόχου.Υπάρχουν τρεις βασικές αλυσίδες, που ονομάζονται αντίστοιχα input, output και forward. Όλα τα πακέτα που εισέρχονται στο μηχάνημα περνάνε από την input αλυσίδα και αυτά που εξέρχονται περνάνε από την output. Η forward αλυσίδα χρησιμοποιείται για τα πακέτα που προορίζονται για διαφορετικό interface δικτύου από αυτό που ελήφθησαν.

Πιο συγκεκριμένα οι κανόνες μπορούν να βασιστούν σε ένα από τα παρακάτω:

- Τον αριθμό πρωτοκόλλου (TCP, UDP ICMP, IGMP)
- Την IP διεύθυνση προέλευσης ή προορισμού,
- Τον αριθμό της πόρτας προέλευσης TCP ή UDP,
- Τον τύπο και κωδικό του ICMP,
- Εάν το πακέτο είναι πακέτο TCP που αρχικοποιεί τη σύνδεση,
- Το interface του δικτύου που φθάνει η αναχωρεί το πακέτο.

Κάθε κανόνας έχει μια target action που δηλώνει τι πρόκειται να συμβεί με το πακέτο. Οι ενέργειες που μπορεί να ακολουθήσουν είναι οι εξής:

- Deny: απόρριψη του πακέτου χωρίς καμία ενημέρωση,
- Redirect: απόρριψη του πακέτου αλλά ενημέρωση με αποστολή ICMP πακέτου,
- Accept: προώθηση του πακέτου,
- Masq: τροποποίηση του πακέτου,

· Redirect: προώθηση του πακέτου σε διαφορετική πόρτα,
Κανόνας που προέρχεται από αλυσίδα που ορίζει ο χρήστης.

• IPfilter

Αυτό το σύστημα φιλτραρίσματος πακέτου βρίσκεται σε UNIX συστήματα όπως τα FreeBSD, OpenBSD και NetBSD καθώς επίσης και σε Solaris.
- Η μέθοδος του packet filtering έχει τα παρακάτω πλεονεκτήματα:

α) Προστασία ενός δικτύου με τη χρήση ενός screening router

β) Το απλό φιλτράρισμα των πακέτων αποτελεί μια γρήγορη και αποδοτική μέθοδο

γ) Επειδή το φιλτράρισμα απαιτεί μόνο τον έλεγχο του header κάθε πακέτου, υπάρχει πολύ μικρή καθυστέρηση στην ολοκλήρωσης της εργασίας ελέγχου, σε αντίθεση με τα proxy συστήματα στα οποία υπάρχει αρκετή καθυστέρηση.

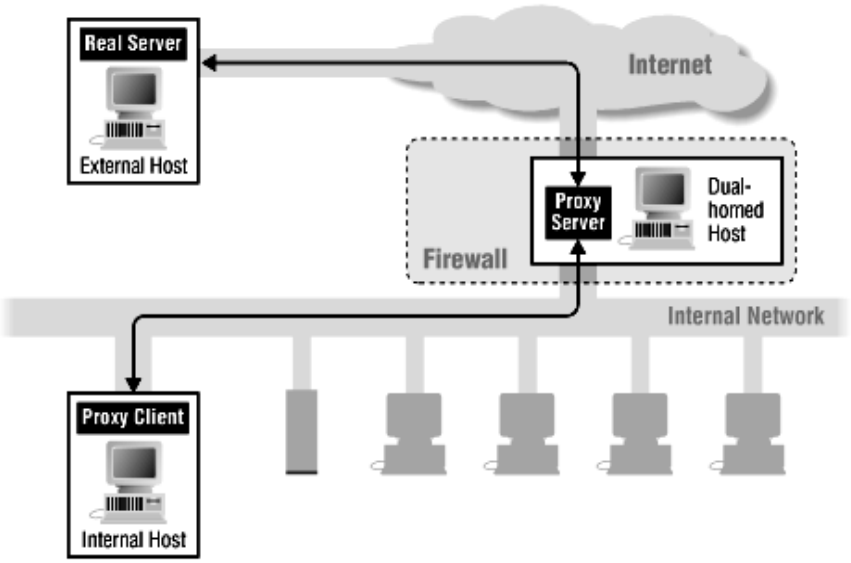
δ) Ευρεία διαθέσιμη μέθοδος

Πολλά προϊόντα τόσο λογισμικού όσο και hardware έχουν δυνατότητες packet filtering.
- Όμως η μέθοδος του packet filtering έχει και μειονεκτήματα:
Υπάρχουν πολλά εργαλεία φιλτραρίσματος που είναι ατελή.
Κάποιες ατέλειες είναι οι παρακάτω:
α) Δυσκολία στην διαμόρφωση των κανόνων που έχουν οριστεί
β) Δυσκολία ελέγχου σωστής λειτουργίας των ρυθμίσεων που έχουν γίνει
γ) Υπάρχει έλλειψη εξειδικευμένων φίλτρων.
Κάποιοι κανόνες δεν είναι δυνατόν να εφαρμοστούν από απλούς δρομολογητές φιλτραρίσματος πακέτων.

2.7.2. Proxy Services

Γενικά με τον όρο proxy services εννοούμε τις εφαρμογές εκείνες που συνήθως τρέχουν σε κάποιον server, δέχονται τις αιτήσεις από κάποιον χρήστη για διάφορες internet υπηρεσίες (όπως FTP και TELNET) και ουσιαστικά αποτελούν τους μεσολαβητές των χρηστών για τη σύνδεση αυτών με τον έξω κόσμο. Οι μεσολαβητές (proxies) που χρησιμοποιούνται για λόγους ασφαλείας τοποθετούνται είτε σε dual-homed host (με το ένα interface να συνδέεται στο εσωτερικό δίκτυο και το άλλο στο εξωτερικό), είτε σε bastion-host που έχουν πρόσβαση στο internet και είναι και είναι προσβάσιμοι από τα εσωτερικά μηχανήματα.

Στο παρακάτω σχήμα (3) φαίνεται ένα proxy σύστημα. Αποτελείται από δύο τμήματα: τον proxy client και τον proxy server. Το σύστημα που τρέχει ο server είναι ένα dual-homed host σύστημα.



Σχήμα 3: Dual-Homed host σαν proxy server

Έτσι ο proxy server δέχεται αιτήσεις από τον proxy client και ανάλογα με τις ρυθμίσεις που έχουν γίνει, σύμφωνα με ην πολιτική ασφαλείας που ακολουθείται, τις απορρίπτει ή τις προωθεί στον real server ο οποίος με τη σειρά του στέλνει τις απαντήσεις στον proxy client.

- **Πως γίνεται το proxying:**

Συνήθως για να δημιουργήσουμε ένα proxy σύστημα απαιτείται:

- Εγκατάσταση κατάλληλου proxy server λογισμικού στην πλευρά του server
- Εγκατάσταση ενός από τα παρακάτω στην πλευρά του client:
  - Proxy-aware application software
  - Proxy-aware operating system software
  - Proxy–aware user procedures
  - Proxy-aware router

· **Αναλυτικά**

I. Proxy-aware application software:

Στη περίπτωση αυτή, το λογισμικό θα πρέπει να γνωρίζει πρώτον, πως θα επικοινωνήσει με τον proxy-server και όχι με τον real-server όταν ο χρήστης ζητήσει μια υπηρεσία και δεύτερον, το πως ο proxy-server θα γνωρίζει με ποιον real-server θα συνδεθεί.

II. Proxy-aware operating system software

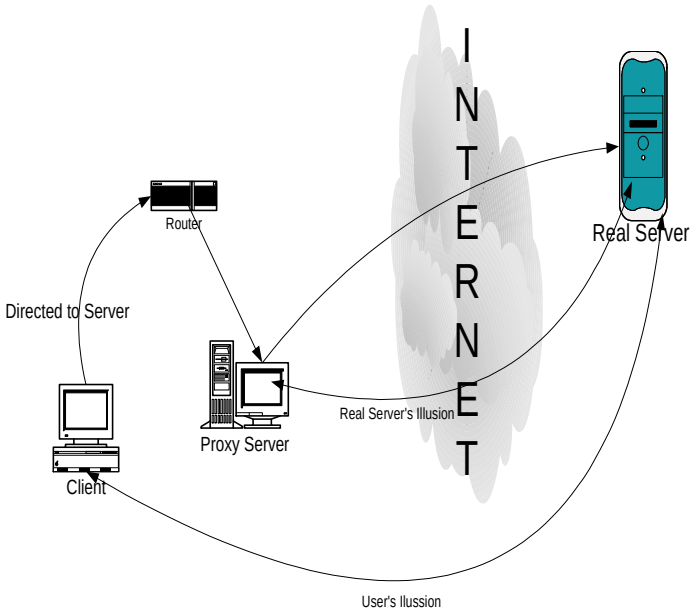
Σε αυτή τη περίπτωση, το λειτουργικό σύστημα που τρέχει ο client τροποποιείται έτσι ώστε οι IP συνδέσεις να ελέγχονται για το αν επιτρέπεται να σταλούν στον proxy-server. Η μέθοδος αυτή στηρίζεται στην δυναμική προσθήκη βιβλιοθηκών όταν τρέχει το πρόγραμμα.

III. Proxy–aware user procedures

Σε αυτή τη περίπτωση, οι proxy-servers είναι σχεδιασμένοι για να υποστηρίζουν συγκεκριμένο λογισμικό στον client και επίσης επιβάλλουν στους χρήστες να ακολουθήσουν συγκεκριμένες διαδικασίες για τη σύνδεση. Έτσι, οι χρήστες λένε στον client να συνδεθεί με τον proxy-server και στη συνέχεια στον server με ποιον host θα συνδεθεί. Για τη σωστή λειτουργία της μεθόδου θα πρέπει οι χρήστες να μάθουν συγκεκριμένες διαδικασίες για κάθε πρωτόκολλο.

IV. Proxy-aware router

Σε αυτή τη περίπτωση, δεν τροποποιείται τίποτα στην πλευρά του client, απλά μεσολαβεί κάποιος δρομολογητής ανάμεσα στον client και τον proxy ή real server και ανάλογα με την πολιτική που ακολουθείται τα πακέτα που προέρχονται από τον client είτε στέλνονται απευθείας στον real-server, είτε απορρίπτονται, είτε στέλνονται στον proxy-server.
Η λύση του proxy-aware router που αποτελεί και την πιο εύκολη για τους χρήστες φαίνεται σχηματικά παρακάτω (σχήμα 4):



Σχήμα 4. Proxy-aware router

2.7.2.1 Τύποι Proxy Servers

- **Application-level μεσολαβητές, έναντι Circuit-level**

Οι μεσολαβητές application-level είναι αυτοί που γνωρίζουν τις εφαρμογές για τις οποίες παρέχουν τις υπηρεσίες τους μεταφράζοντας το application πρωτόκολλο σε αντίθεση με τους circuit-level μεσολαβητές που δημιουργούν ένα κύκλωμα ανάμεσα στον client και τον server χωρίς να κατανοούν το

application πρωτόκολλο.
Το πλεονέκτημα των μεσολαβητών circuit-level, είναι ότι παρέχουν υπηρεσίες σε πληθώρα πρωτοκόλλων. Όμως έχουν και μειονεκτήματα αφού δεν παρέχουν ολοκληρωμένο έλεγχο για το τι συμβαίνει μέσα στον μεσολαβητή.

- **Generic μεσολαβητές, έναντι Dedicated μεσολαβητών**

Η διαφορά μεταξύ τους είναι ότι οι dedicated τύπου μεσολαβητές εξυπηρετούν ένα μόνο πρωτόκολλο ενώ οι άλλοι εξυπηρετούν πολλά. Πρακτικά οι dedicated μεσολαβητές ανήκουν στην κατηγορία των application-level ενώ οι generic ανήκουν στους circuit-level.

- **Έξυπνοι μεσολαβητές(Intelligent Proxy Servers)**

Οι μεσολαβητές που έχουν επιπλέον δυνατότητες, πέρα από το να μεσολαβούν απλά για την προώθηση πακέτων ονομάζονται “έξυπνοι” μεσολαβητές. Για παράδειγμα, σχεδόν όλοι οι HTTP proxy-servers κρατούν στην μνήμη τους δεδομένα, έτσι ώστε να γίνονται γρηγορότερα οι νέες συνδέσεις που έχουν κοινά χαρακτηριστικά με παλαιότερες.

- **Μεσολάβηση χωρίς Proxy-Server**

Κάποιες υπηρεσίες, όπως SMTP, NNTP, και NTP, υποστηρίζουν από μόνες τους το proxying. Τέτοιες υπηρεσίες είναι σχεδιασμένες έτσι ώστε οι συναλλαγές να γίνονται ανάμεσα σε servers και όχι από κάποιον client σε έναν τελικό server. Για παράδειγμα το NNTP προωθεί τα μηνύματα σε όλους τους γειτονικούς servers. Έτσι, κάθε ενδιάμεσος server δρα στην πραγματικότητα ως μεσολαβητής.
Εάν, για παράδειγμα, εξετάσουμε τις επικεφαλίδες(headers) του internet mail που προορίζονται στο εσωτερικό δίκτυο, θα δούμε ότι πολύ λίγα είναι τα μηνύματα που ταξιδεύουν απευθείας από τον αποστολέα προς τον παραλήπτη. Συνήθως περνάνε διαμέσου τεσσάρων συστημάτων:

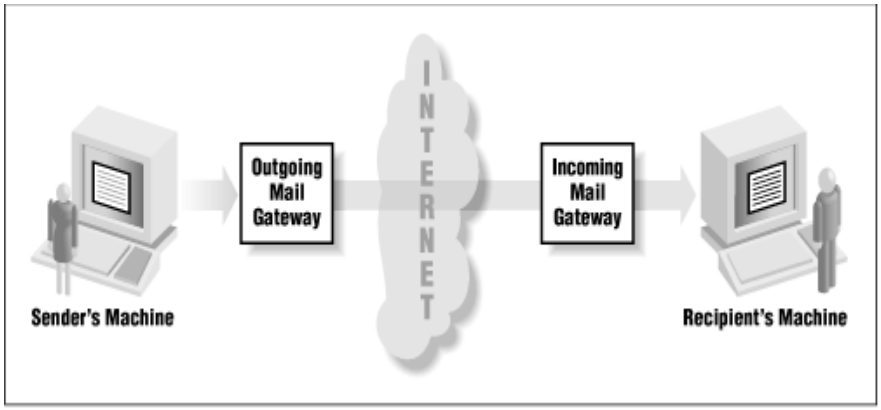
1.) Το μηχάνημα του αποστολέα

2.) Την εξερχόμενη πύλη (outgoing mail gateway)στο site του αποστολέα

3.) Την αντίστοιχη εισερχόμενη πύλη (ingoing mail gateway)στο site του παραλήπτη

4.) Τέλος, το μηχάνημα του παραλήπτη

Έτσι, κάθε ένας από τους ενδιάμεσους servers δρα ως proxy-server.
Στο παρακάτω σχήμα(5) φαίνεται η διαδικασία αυτή:



Σχήμα 5. Υλοποίηση proxying χωρίς proxy server

ü Πλεονεκτήματα των Proxy Servers:

Η χρήση υπηρεσιών μεσολάβησης έχει τα παρακάτω πλεονεκτήματα:

I. Παρέχουν τη δυνατότητα βελτιώσεις απόδοσης του συστήματος μέσω caching.

   Οι μεσολαβητές έχουν τη δυνατότητα να διατηρούν αντίγραφα των δεδομένων που ζητούνται από τους χρήστες. Έτσι εάν ο αριθμός των «αιτήσεων» των χρηστών για μια υπηρεσία είναι μεγάλος τότε το caching που εκτελείται από τους μεσολαβητές διευκολύνει στην αποσυμφόρηση του δικτύου.

II. Δυνατότητα έξυπνου φιλτραρίσματος

Επίσης οι μεσολαβητές επικεντρώνονται περισσότερο στο περιεχόμενο των πακέτων έχουν τη δυνατότητα να κάνουν πιο αξιόπιστο φιλτράρισμα σε σχέση με αυτό που κάνουν τα συστήματα φιλτραρίσματος πακέτων. Για παράδειγμα, οι μεσολαβητές έχουν τη δυνατότητα φιλτραρίσματος HTTP πακέτων με βάση το περιεχόμενο του πακέτου. Έτσι είναι ικανοί να αποτρέψουν την JAVA ή JAVASCRIPT σε κάποια πακέτα. Γενικά είναι πιο αποτελεσματικοί στην προστασία από ιούς σε σχέση με τα συστήματα φιλτραρίσματος πακέτων.

III. Παρέχουν authentication σε επίπεδο χρήστη

Επειδή ένα σύστημα μεσολάβησης συμμετέχει ενεργά σε μία σύνδεση, είναι εύκολο γι' αυτό να λάβει μέτρα που αφορούν το χρήστη.

IV. Παρέχουν αυτόματα προστασία από αδύνατες ή λανθασμένες IP εφαρμογές

Αφού κάποιος μεσολαβητής είναι τοποθετημένος ανάμεσα σε έναν client και το internet, γεννά εξ' ολοκλήρου νέα πακέτα για τον client. Έτσι, προστατεύει τους clients από κακόβουλα IP πακέτα.

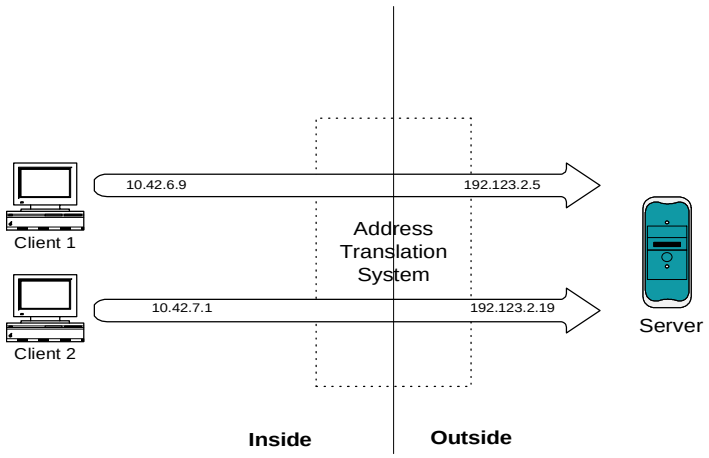
— Υπάρχουν όμως και κάποια μειονεκτήματα. Αυτά είναι:

I. Κάποιοι μεσολαβητές απαιτούν διαφορετικούς servers για κάθε υπηρεσία

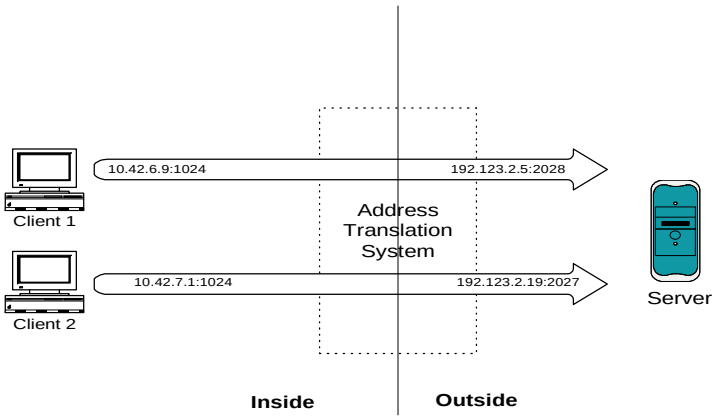
II. Συνήθως για την εγκατάσταση υπηρεσιών μεσολάβησης, απαιτούνται επιπλέον τροποποιήσεις στους clients καθώς επίσης και σε συγκεκριμένες εφαρμογές

2.7.3. Network Address Translation

Η μέθοδος αυτή από μόνη της δεν παρέχει ασφάλεια αλλά βοηθά στην απόκρυψη των διευθύνσεων του εσωτερικού δικτύου από τον έξω κόσμο και επίσης οδηγεί την κίνηση να περάσει από ένα και μοναδικό σημείο (choke point) προσφέροντας με αυτόν τον τρόπο καλύτερη παρακολούθηση των πακέτων που εισέρχονται και εξέρχονται προς και από το εσωτερικό δίκτυο. Ειδικότερα, κάθε πακέτο που στέλνεται από ένα εσωτερικό μηχάνημα προς το internet, εμφανίζεται με διαφορετική διεύθυνση προέλευσης και σε κάθε εισερχόμενο πακέτο, μετατρέπεται η διεύθυνση προορισμού του με το σύστημα NAT, στην πραγματική εσωτερική διεύθυνση του μηχανήματος.
Επιπλέον το σύστημα NAT έχει τη δυνατότητα να τροποποιεί την διεύθυνση της πόρτας προορισμού και προέλευσης των πακέτων. Η μέθοδος αυτή ονομάζεται Port Address Translation (PAT).
Στα παρακάτω σχήματα(6 και 7) φαίνονται τα συστήματα NAT και PAT:



Σχήμα 6. Network Address Translation



Σχήμα 7. Port and Address Translation

♦ Υπάρχουν διάφοροι τρόποι που χρησιμοποιεί το σύστημα NAT για την μετάφραση ανάμεσα στις εσωτερικές και εξωτερικές διευθύνσεις :

⇒ Χρησιμοποίηση μιας μόνο διεύθυνσης για την μετάφραση κάθε εσωτερικής διεύθυνσης. Ο τρόπος αυτός επιβραδύνει τις συνδέσεις και συνήθως εφαρμόζεται προσωρινά.

⇒ Δυναμική κατανομή διευθύνσεων κάθε φορά που κάποιο εσωτερικό σύστημα ξεκινά μια σύνδεση προς τον έξω κόσμο, χωρίς όμως την τροποποίηση των αριθμών της πόρτας. Ο τρόπος αυτός περιορίζει τον αριθμό των ταυτόχρονων συνδέσεων στον έξω κόσμο. Ο αριθμός αυτός εξαρτάται από τον αριθμό των διαθέσεων διευθύνσεων.

⇒ Δυναμική κατανομή διευθύνσεων με την δυνατότητα τροποποίησης των αριθμών πόρτας κάθε φορά που αρχικοποιείται μια εσωτερική σύνδεση. Ο τρόπος αυτός αποτελεί και τον καταλληλότερο και αποδοτικότερο.

ü ΠΛΕΟΝΕΚΤΗΜΑΤΑ

I. Καλύτερος έλεγχος όσο αφορά τις εξερχόμενες συνδέσεις

Σε πολλές περιπτώσεις, υπάρχουν hosts οι οποίοι έχουν διευθύνσεις που θεωρούνται ακατάλληλες για τον έξω κόσμο. Έτσι εάν κάποιος host βρει κάποιον τρόπο να συνδεθεί στο διαδίκτυο χωρίς να αλλάξει την διεύθυνση του(μέσω NAT) είναι πιθανό η σύνδεση αυτή να αποτύχει.

II. Το σύστημα NAT είναι δυνατό να περιορίσει την εισερχόμενη κίνηση

Στην περίπτωση του δυναμικού NAT εάν ο επιτιθέμενος δεν δράσει άμεσα θα χάσει οποιαδήποτε πληροφορία σχετικά με το host που αρχικοποίησε τη σύνδεση αφού πλέον ολόκληρη η διεύθυνση θα έχει πλήρως εξαφανιστεί ή θα έχει δοθεί σε άλλον host.

Γενικά το σύστημα NAT βοηθά στην πλήρη απόκρυψη της διαμόρφωσης του εσωτερικού δικτύου
Το σύστημα αυτό δεν αποκαλύπτει τον αριθμό των υπολογιστικών μηχανημάτων που βρίσκονται στο δίκτυο αλλά ούτε τον τρόπο της συνδεσμολογίας τους.

– ΜΕΙΟΝΕΚΤΗΜΑΤΑ

I. Η δυναμική κατανομή των νέων διευθύνσεων απαιτεί και γνώση της κατάστασης της σύνδεσης που τις περισσότερες φορές δεν είναι διαθέσιμη

Για παράδειγμα είναι εύκολο για ένα σύστημα NAT να γνωρίζει πότε κάποιος host έχει σταματήσει μια TCP σύνδεση όμως δεν είναι σε θέση να γνωρίζει εάν ένα UDP πακέτο είναι μέρος μιας τρέχουσας σύνδεσης ή αποτελεί ένα μεμονωμένο γεγονός. Αυτό σημαίνει ότι το σύστημα NAT θα πρέπει να υποθέσει το χρόνο που θα κρατήσει μεταφρασμένη κάποια διεύθυνση. Εάν δεν υποθέσει σωστά τότε υπάρχει ο κίνδυνος να χαθούν πακέτα και συνεπώς χρήσιμες πληροφορίες.

II. Κίνδυνος παρεμβολής στο σύστημα packet filtering

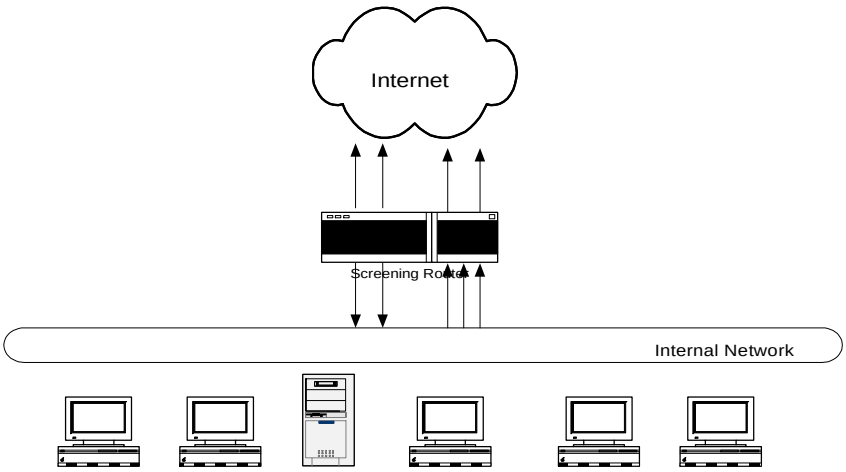
Είναι γνωστό ότι τα συστήματα φιλτραρίσματος πακέτων λαμβάνουν υπόψη τον αριθμό πόρτας προέλευσης και προορισμού κάθε πακέτου για να μάθουν το πρωτόκολλο που χρησιμοποιείται. Όμως με τη δυναμική κατανομή αριθμών πόρτας που γίνεται με το NAT σύστημα είναι δυνατό να υπάρχει πρόβλημα αποδοχής κάποιου πακέτου. Για παράδειγμα εάν πακέτα με αριθμό πόρτας πάνω από 1023(συνήθως πόρτες που χρησιμοποιούνται από τους clients) μεταφραστούν σε πόρτες μικρότερες από 1023 τότε υπάρχει κίνδυνος τα πακέτα αυτά να χαθούν.

2.8. Αρχιτεκτονικές των Firewall

Τώρα θα εξετάσουμε διάφορες αρχιτεκτονικές εγκατάστασης ενός firewall καθώς θα αναφερθούμε στα πλεονεκτήματα και τα μειονεκτήματα αυτών.

2.8.1. Αρχιτεκτονική “Single-Box”

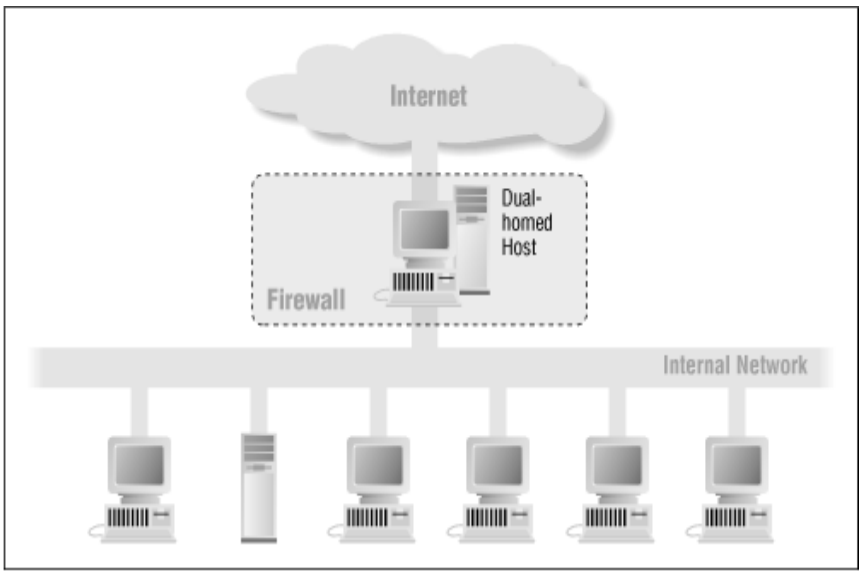
Η αρχιτεκτονική τέτοιας μορφής στηρίζεται στη χρησιμοποίηση ενός και μόνο αντικειμένου ως τοίχου προστασίας. Γενικά το πλεονέκτημα σε αυτή την περίπτωση είναι ότι έχεις ένα μόνο σημείο από το οποίο περνά ολόκληρη η κίνηση προς το site της εταιρείας και συνεπώς υπάρχει η δυνατότητα να το ελέγχεις και να το διαμορφώνεις με το βέλτιστο τρόπο. Αντίθετα σοβαρό μειονέκτημα είναι το ότι δεν υπάρχει ασφάλεια σε βάθος και σε περίπτωση που παραβιαστεί το σημείο αυτό δε θα υπάρχει εναλλακτικός τρόπος προστασίας του εσωτερικού δικτύου της εταιρείας.



Σχήμα 1. Screening Router

2.8.2. Αρχιτεκτονική Dual-Homed-Host

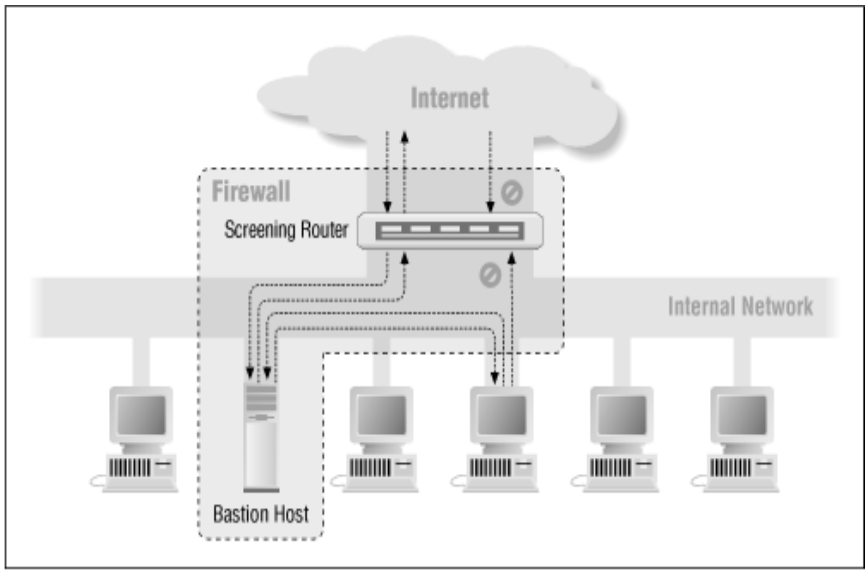
Ένα τερματικό dual-homed θεωρείται αυτό που έχει δύο κάρτες δικτύου και για να χρησιμοποιηθεί ως firewall θα πρέπει τα ip πακέτα από το ένα δίκτυο να μην δρομολογούνται άμεσα στο άλλο δίκτυο. Έτσι τα συστήματα στο εσωτερικό του firewall θα μπορούν να επικοινωνήσουν απευθείας με το dual-homed host αλλά όχι και με τον έξω κόσμο και τα συστήματα στον έξω κόσμο θα μπορούν να επικοινωνούν μόνο με το dual-homed host και όχι με τα συστήματα στο εσωτερικό δίκτυο.



Σχήμα 2. Dual-Homed Host Αρχιτεκτονική

2.8.3. Αρχιτεκτονικές “Screened-Host”

Ενώ στην αρχιτεκτονική dual-homed host στο σύστημα που παρέχει τις υπηρεσίες είναι επικολλημένα τόσο το εσωτερικό όσο και το εξωτερικό δίκτυο στην αρχιτεκτονική screened host στο σύστημα που παρέχει τις υπηρεσίες είναι επικολλημένο μόνο το εσωτερικό δίκτυο.

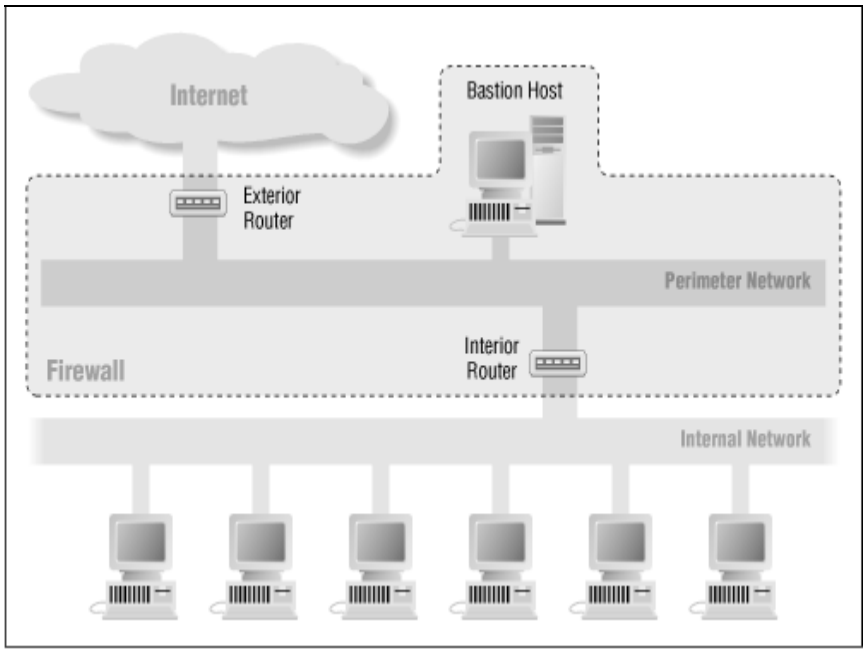


Σχήμα 3. Screened Host Αρχιτεκτονική

2.8.4. Αρχιτεκτονικές “Screened Subnet”

Η αρχιτεκτονική αυτή προσθέτει ένα ακόμα επίπεδο ασφαλείας σε σχέση με την προηγούμενη αρχιτεκτονική προσθέτοντας στην ουσία ένα περιμετρικό δίκτυο το οποίο απομονώνει ακόμη περισσότερο το εσωτερικό δίκτυο από το internet. Από τη φύση του ο bastion host είναι το σύστημα που είναι περισσότερο ευαίσθητο σε ολόκληρο το δίκτυο. Όταν κάποιος γνωρίζει ότι με το να εισβάλλει μέσα σε αυτό θα αποκτήσει και άμεση πρόσβαση στο δίκτυο είναι φυσιολογικό να επικεντρώσει τις προσπάθειες του στο πως θα το κατακτήσει. Έτσι η αρχιτεκτονική αυτή έρχεται κατά κάποιο τρόπο να απομονώσει το σύστημα μέσα σε ένα περιμετρικό δίκτυο με σκοπό να μη θεωρείται πλέον από τους επιτιθέμενους το πιο κρίσιμο σημείο του δικτύου.

Η αρχιτεκτονική screened subnet είναι κατάλληλη για τις περισσότερες των περιπτώσεων.



Σχήμα 4. Screened Subnet Αρχιτεκτονική

2.8.5. Αρχιτεκτονικές με Πολλαπλα Screened-Subnets

Κάποια δίκτυα ίσως χρειαστούν περισσότερα από ένα screened subnet.

- Split-Screened Subnet
- Independent Screened Subnets

3. Πρωτόκολλα Ασφάλειας

3.1. Internet Security Protocol (IPSec)(Πρωτόκολλο ασφάλειας διαδικτύου)

Η ομάδα IP Security (IPSec) της Internet Engineering Task Force (IETF) είναι υπεύθυνη για τον ορισμό προτύπων και πρωτοκόλλων που σχετίζονται με την

ασφάλεια στο Internet. Τα VPN δίκτυα χρησιμοποιούν αυτά τα πρότυπα ως ένα μέρος των δικών τους μέτρων ασφαλείας που παρέχουν στους χρήστες τους. Η IPSec ομάδα όρισε την δομή του IP πακέτου και υλοποίησε διάφορες secure associations(ασφαλής συνδέσεις) (SA) οι οποίες από τον Νοέμβριο του 1998 έχουν καθιερωθεί ως πρότυπα και χρησιμοποιούνται στις VPN επικοινωνίες. Το IPSec ορίζει ένα σύνολο πρωτοκόλλων και κρυπτογραφικών αλγορίθμων για δημιουργία ασφαλούς IP κυκλοφορίας μεταξύ IPSec gateways(πύλες). Παρέχει τις βασικές λειτουργίες και ένα αριθμό προϊόντων τα οποία έχουν πιστοποιηθεί σαν interoperable.

Το IPSec πρωτόκολλο απαιτεί πριν από κάθε επικοινωνία να δημιουργηθεί μία ασφαλής συσχέτιση (Secure Association - SA) μεταξύ δύο VPN κόμβων ή gateways. Αυτή η ασφαλής συσχέτιση μεταξύ των δύο κόμβων ελέγχει όλες τις παραμέτρους που εξασφαλίζουν μία ασφαλή επικοινωνία. Δηλαδή ελέγχει τις υπηρεσίες των επιπέδων μεταφοράς και εφαρμογής και κάνει authentication, θέτει διάφορα στοιχεία τα οποία θα διασφαλίσουν την μελλοντική επικοινωνία μεταξύ των δύο τερματικών hosts συμπεριλαμβανομένων και των περιπτώσεων όπου το πακέτο κρυπτογραφείται και πιστοποιείται και από τους δύο hosts.

3.1.1 Προβλήματα που παρουσιάζονται στο IPSec

Γενικά το IPSec μπορούμε να πούμε ότι δεν αντιμετωπίζει αρκετά προβλήματα. Ένα από τα αυτά είναι η περίπτωση όπου τα κλειδιά είναι στατικά κατά την διάρκεια της επικοινωνίας και δεν υπάρχει μηχανισμός για ανταλλαγή αυτών των κλειδιών. Ένα άλλο σημαντικό πρόβλημα για το IPSec είναι η δυσκολία χειρισμού του μεγάλου αριθμού των κρυπτογραφικών κλειδιών στα μεγάλα δίκτυα. Μία λύση σε αυτό το πρόβλημα είναι το Certificate Enrollment Protocol (CEP) (πρωτόκολλο πιστοποιημένης εγγραφής)το οποίο έχει αναπτυχθεί από την Cisco και την VeriSign και επιτρέπει την ανταλλαγή μεγάλου αριθμού κλειδιών.
Μέχρι σήμερα έχουν γίνει αρκετές αλλαγές στο αρχικό IPSec πρότυπο. Δεδομένου ότι πολλοί χρήστες των VPN

χρησιμοποιούν dial-up συνδέσεις στο δίκτυο το IPSec χρειάζεται να γνωρίζει πώς να διαχειρίζεται τις δυναμικές διευθύνσεις. Έτσι μία από αυτές τις αλλαγές είχε σαν κύριο στόχο να υποστηρίξει δυναμικές client διευθύνσεις.

3.2. Mobile IP και IPsec

Τα πρωτόκολλα στα οποία πρέπει να στηρίζεται ένα MVPN είναι το Mobile IP και το IPSec. Η χρήση του πρωτοκόλλου Mobile IP πρόκειται να καθιερώσει το δίκτυο προσπελάσιμο έτσι ώστε οι κινητοί χρήστες να μπορούν να δοκιμάσουν να συνδεθούν ανεξάρτητα από πού αυτοί βρίσκονται. Το πρωτόκολλο IPsec είναι το πρωτόκολλο ασφάλειας που προτιμάται για την μεγαλύτερη πλειοψηφία των σημερινών VPN δικτύων.

3.2.1.Χρήση του IPSec στο Mobile IP

Η χρήση ESP του πρωτοκόλλου IPSec στο Mobile IP θα προστατεύσει τα ανακατευθυνόμενα πακέτα από τις επιθέσεις που δέχονται και θα βοηθήσει αυτά τα πακέτα να διαπεράσουν το σπίτι και τα ξένα δίκτυα που επισκέπτονται οι κινητοί κόμβοι.

3.3. Ψηφιακή Πιστοποίηση

3.3.1. Public Key Infrastructure (PKI)

Το PKI είναι ένα σύστημα ψηφιακών πιστοποιήσεων (digital certificates), πιστοποιήσεων εξουσιών (authorities certificates), πιστοποιήσεων διαχείρισης υπηρεσιών (certificate management services), και directory services (LDAP, X.500) το οποίο εξακριβώνει την ταυτότητα και την εξουσία του κάθε χρήστη που λαμβάνει μέρος σε κάθε συναλλαγή στο Διαδίκτυο.
Μερικές χρήσεις του PKI είναι:
─Authentication και authorization
─Privacy και confidentiality
─Integrity of data
─Nonrepudiation

─Directory Services π.χ X.500, LDAP
─Document Transmission
─Legal και financial transaction
─Document archive και retrieval

Το PKI έχει υλοποιηθεί για εφαρμογές οι οποίες υποστηρίζουν ασφάλεια στις υπηρεσίες του Internet όπως για παράδειγμα email, έγγραφα στο WWW και ηλεκτρονικό εμπόριο. Οι πληροφορίες οι οποίες περιέχονται σε ένα PKI πιστοποιητικό (certificate) περιλαμβάνουν :

─Η identity του certificate holder
─Το serial number του certificate
─Τα expiration dates του certificate
─Αντίγραφο του public key και την digital signature του χρήστη
─Το όνομα του certificate authority και την digital signature του

3.4. Layer 2 Forwarding Protocol (L2F)

Το L2F είναι ένα από τα πρωτόκολλα που χρησιμοποιούνται σήμερα στα VPN σε συνδυασμό με το PPTP. Λόγω της μεγάλης ανάπτυξης των dial-up υπηρεσιών και την παροχή πολλών διαφορετικών πρωτοκόλλων χρειαζόταν ένας τρόπος για να δημιουργείται ένα εικονικό dial-up (virtual) σενάριο όπου οποιοδήποτε από τα μη-IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το Internet. Οι χρήστες μπορούν να κάνουν μία PPP ή SLIP σύνδεση σε ένα dial-up ISP παροχέα υπηρεσιών και χρησιμοποιώντας το L2F πρωτόκολλο να συνδεθούν στα μηχανήματα της εταιρείας τους.
Ορισμένα από τα οφέλη που προσφέρει το L2F είναι :

- Ανεξαρτησία πρωτοκόλλων (IPX, SNA)
- Authentication (PPP, CHAP, TACACS)
- Διαχείριση διευθύνσεων
- Δυναμικά και ασφαλή tunnels
- Accounting
- Ανεξαρτησία των media
- Από κοινού L2F tunneling και τοπική πρόσβαση στο Internet

Σε μία τυπική εγκατάσταση ο χρήστης κάνει μία PPP ή

άλλη παρόμοια σύνδεση στον ISP και κατά την διάρκεια της αίτησης το NAS, χρησιμοποιώντας το λογισμικό του L2F, αρχικοποιεί ένα tunnel προς τον προορισμό του χρήστη. Στη συνέχεια, ο προορισμός απαιτεί το password του χρήστη και αφού γίνει authorized παραχωρείται στο χρήστη η IP διεύθυνση σαν μία τυπική dial-up απομακρυσμένη πρόσβαση.

3.5. Point-to-Point Tunneling Protocol (PPTP)

Το PPTP είναι ένας συνδυασμός του Point-to-Point Protocol και του Transmission Control Protocol / Internet Protocol (TCP/IP). Το PPTP συνδυάζει τα χαρακτηριστικά του PPP (π.χ privacy με συμπίεση πακέτων δεδομένων) και του TCP/IP (κυρίως τη δυνατότητα για δρομολόγηση των πακέτων στο Internet). Μαζί με το IPSec είναι ένα από τα κύρια VPN πρωτόκολλα που χρησιμοποιούνται σήμερα.
Το PPTP μπορεί να πάρει πακέτα όπως IP, IPX, NetBios, SNA και να τα μετατρέψει σε ένα καινούριο IP πακέτο για μεταφορά. Χρησιμοποιεί το Generic Routing Protocol (GRE) για μεταφορά των PPP πακέτων. Χρησιμοποιεί επίσης encryption για encapsulated δεδομένα τα οποία παρέχει για authentication. Η κίνηση του PPTP αποτελείται από δύο είδη πακέτων για διαφορετικούς τύπους δεδομένων: data packets και control packets. Τα control packets χρησιμοποιούνται για signaling ενώ τα data packets για να μεταφέρουν τα δεδομένα του χρήστη. Τα data packets είναι πακέτα τα οποία έχουν υποστεί την διαδικασία του encapsulation χρησιμοποιώντας το

3.6. Internet Generic Routing Encapsulation Protocol Version 2 (GRE v2)

Η PPTP σύνδεση ξεκινά σαν ένα handshake μεταξύ δύο απομακρυσμένων σημείων με σκοπό την επίτευξη συμφωνίας στο συμπιεστικό σχήμα και στη μέθοδο για encapsulation που θα χρησιμοποιηθεί. Κατά την διάρκεια της επικοινωνίας αυτά τα πακέτα μπορούν, αν απαιτηθει, να τμηματοποιηθούν και ένα PPP header προσθέτει ένα serialization αριθμό για την εξακρίβωση χαμένων

πακέτων.

Τα PPTP και IPSec μπορούν να επιτύχουν παρόμοια αποτελέσματα. Μπορούμε να έχουμε ένα IPSec client για την εγκατάσταση ασφαλούς session σε ένα firewall και την δημιουργία ενός VPN ή να έχουμε ένα PPTP client για την εγκατάσταση ενός session στο firewall. Όμως, το PPTP χρειάζεται ένα NT-based firewall αφού τρέχει μόνο σε NT servers. Το PPTP εμφανίζεται με δύο τρόπους, ο πρώτος είναι ο υποχρεωτικός τρόπος όπου η PPTP σύνδεση γίνεται στο σημείο σύνδεσης του ISP. Επομένως, ο ISP θα χρειαστεί ένα ειδικό επεξεργαστή για να χειριστεί τις PPTP συνδέσεις. Ο δεύτερος τρόπος είναι ο εθελοντικός τρόπος κατά τον οποίο η PPTP σύνδεση γίνεται στο άκρο, για παράδειγμα client-to-server.

Το PPTP αποτελείται από τρία είδη επικοινωνίας:

- **PPTP σύνδεση**: Αυτή γίνεται όταν ο client εγκαταστήσει ένα PPP ή ISDN σύνδεσμο με τον ISP του.
- **PPTP σύνδεση ελέγχου (control connection):** Χρησιμοποιώντας το Internet ο χρήστης δημιουργεί την PPTP σύνδεση στον VPN server και θέτει τα PPTP χαρακτηριστικά του tunnel
- **PPTP data tunnel:** Ο client και ο server επικοινωνούν μεταξύ τους μέσω του κρυπτογραφημένου tunnel.

Η ασφάλεια στο PPTP είναι ολοκληρωμένη με το Windows NT RAS security. Η επικοινωνία μεταξύ απομακρυσμένων χρηστών και το ιδιωτικό δίκτυο της εταιρείας τους γίνεται με RAS κρυπτογράφηση και πιστοποίηση. Τα πρωτόκολλα πιστοποίησης που χρησιμοποιούνται είναι τα PAP, CHAP και MS-CHAP. Τα πρωτόκολλα κρυπτογράφησης είναι κλειδιών των 40-bit όπως RSA-RC4 και DES. Η 128-bit κρυπτογράφηση είναι διαθέσιμη μόνο για χρήση στις ΗΠΑ και Καναδά.

3.7. Layer 2 Tunneling Protocol (L2TP)

Λόγω του ότι μεγάλες εταιρείες όπως η Microsoft, Ascend και 3Com, δούλευαν με το PPTP ενώ η Cisco με το L2F αποφάσισαν για λόγους συμβατότητας να ορίσουν ένα νέο πρότυπο, το L2TP το οποίο είναι το αποτέλεσμα της συγχώνευσης του PPTP και του L2F. Το L2TP παρέχει συμπίεση βασισμένη στο λογισμικό η οποία συμπυκνώνει τα πακέτα των χρηστών. Επίσης, ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης. Το L2TP χρησιμοποιεί δύο συναρτήσεις: την client-like line server η οποία αναφέρεται ως LAC και είναι ένας L2TP συγκεντρωτής πρόσβασης και τον server-side network server ο οποίος καλείται LNS. Όταν ένα PC κάνει PPP σύνδεση στον ISP, μία LAC συνάρτηση αρχικοποιεί το tunnel, προσθέτει διάφορους headers στο PPP payload και εγκαθιδρύει το tunnel στην LNS τερματική συσκευή – αυτή η συσκευή μπορεί να είναι router, server ή συσκευή πρόσβασης. Αφού έχει εγκαθιδρυθεί το tunnel, εγκαθίσταται ένας μηχανισμός πιστοποίησης του χρήστη για να πιστοποιείται η ταυτότητα των χρηστών. Επίσης, το L2TP χρησιμοποιεί control μηνύματα για την βελτιστοποίηση του tunnel.

Το L2TP είναι ένα επίπεδο-2 πρωτόκολλο σχεδιασμένο για το encapsulation στο επίπεδο-2. Επομένως, το IPSec το οποίο είναι ένα πρωτόκολλο επιπέδου-3 μπορεί να χρησιμοποιηθεί μαζί με το L2TP για περισσότερη ασφάλεια (στην πραγματικότητα αυτό συνίσταται).

3.8. Secure Wide Area Network (S/WAN)

Το Secure Wide Area Network (S/WAN) πρωτόκολλο είναι ένα πρωτόκολλο το οποίο παρέχει interoperability. Ακόμη αυτό το πρωτόκολλο δεν έχει υλοποιηθεί. Αν γίνει αποδεκτό και υλοποιηθεί από τις εταιρίες, θα επιτρέψει σε διάφορους οργανισμούς να διασταυρώσουν και αν ταιριάξουν προϊόντα από διάφορες εταιρίες για να δημιουργήσουν κρυπτογραφημένα tunnels. Σκοπός του είναι να βάλει την ασφάλεια όσο πιο χαμηλά γίνεται στο

επίπεδο OSI. Το S/WAN περιλαμβάνει όλους τους γνωστούς αλγορίθμους συμπεριλαμβανομένων των RSA, DES, RC4 και RC5, και κλειδιά των 40 και 128 bits. Το Internet Security Protocol (IPSec) δεν προτείνει κάποιους συγκεκριμένους κρυπτογραφικούς και πιστοποιητικούς αλγορίθμους για να χρησιμοποιηθούν. Επομένως, ακόμη και αν πολλές εταιρίες παροχής VPN υποστηρίζουν IPSec, μπορεί το δίκτυο να μην είναι συμβατό λόγω των κρυπτογραφικών και πιστοποιητικών αλγορίθμων που έχουν χρησιμοποιηθεί. Έτσι το S/WAN βρίσκεται στο κάτω σημείο του επιπέδου όπου βρίσκονται τα πρωτόκολλα κρυπτογράφησης. Για παράδειγμα το SSL-SOCKS θα βρίσκεται στην κορυφή του επιπέδου που βρίσκεται το S/WAN. Έτσι αν όλοι οι vendors υποστηρίξουν το S/WAN, τότε θα έχουμε VPN interoperability με τους διάφορους vendors που υποστηρίζουν το IPSec. Δυστυχώς, αυτό θα αργήσει να γίνει γιατί υπάρχουν αρκετοί vendors που δεν υποστηρίζουν το IPSec.

4. Διαχείριση ασφάλειας στα VPN

4.1.VPN Policy

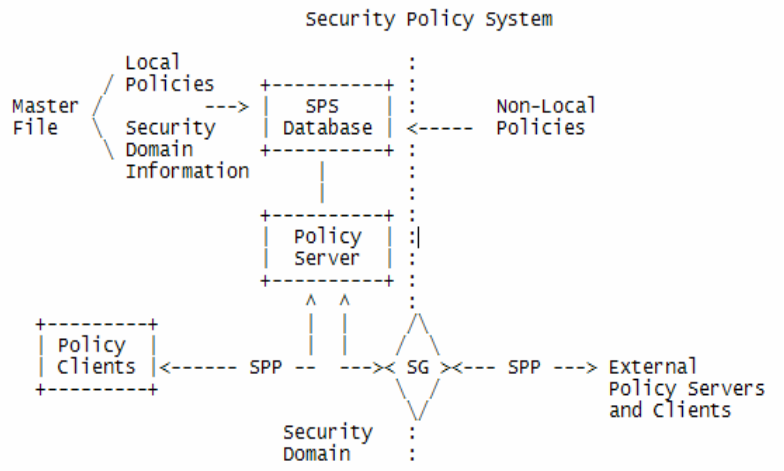
Η **Internet Engineering Task Force [IETF]** καθόρισε το πολιτικό σύστημα ασφάλειας Security Policy System [SPS] το οποίο είναι μια διανεμημένη βάση δεδομένων των πολιτικών πληροφοριών ασφάλειας. Παρέχει τους μηχανισμούς που απαιτούνται για την ανακάλυψη, την πρόσβαση και την επεξεργασία των πολιτικών πληροφοριών ασφάλειας των οικοδεσποτών, των υποδικτύων ή των δικτύων μιας περιοχής ασφάλειας. Σε αυτήν την πολιτική συστημάτων οι πελάτες και οι κεντρικοί υπολογιστές ανταλλάσσουν τις πληροφορίες χρησιμοποιώντας το πολιτικό πρωτόκολλο ασφάλειας Security Policy Protocol [SPP]. Το πρωτόκολλο καθορίζει πώς οι πολιτικές πληροφορίες ανταλλάσσονται, υποβάλλονται σε επεξεργασία, και προστατεύονται από

τους πελάτες και τους κεντρικούς υπολογιστές.

4.1.1 Security Policy System

Το σύστημα διαχείρισης ασφάλειας είναι ένα διανεμημένο σύστημα που παρέχει στους οικοδεσπότες και τις πύλες ασφάλειας και τις πληροφορίες της διαχείρισης ασφαλείας που απαιτούνται για να καθιερώσουν μια ασφαλή end-to-end επικοινωνία μέσω των ενδεχομένως πολλαπλάσιων πυλών ασφάλειας. Το σύστημα διαχείρισης ασφάλειας παρέχει έναν ή περισσότερους αυτοματοποιημένους μηχανισμούς για τους οικοδεσπότες για να ανακαλύψει τις αρχικές και δευτεροβάθμιες πύλες ασφάλειας σχετικές σε μια end-to-end επικοινωνία. Χρησιμοποιώντας το πολιτικό σύστημα ασφάλειας, οι οικοδεσπότες μπορούν να επικυρώσουν την ταυτότητα των πυλών ασφάλειας και να ελέγξουν ότι οι πύλες εξουσιοδοτούνται για να αντιπροσωπεύσουν τον οικοδεσπότη πηγής ή προορισμού.

Το SPS αποτελείται από τους πολιτικούς κεντρικούς υπολογιστές (Policy Servers PS), τους πολιτικούς πελάτες (Policy Clients PC), τα κύρια αρχεία (Master Files) και τις βάσεις δεδομένων SPS. Τα κύρια αρχεία περιέχουν τις τοπικές πολιτικές και άλλες ιδιαίτερες πληροφορίες για μια περιοχή ασφάλειας. Οι τοπικές πολιτικές πληροφορίες που συνδυάζονται με τις μη-τοπικές πολιτικές (πολιτικές έξω από τα όρια της περιοχής ασφάλειας) διαμορφώνουν τις βάσεις δεδομένων SPS. Οι πολιτικοί κεντρικοί υπολογιστές λαμβάνουν τα μηνύματα αιτήματος από τους πολιτικούς πελάτες και άλλους πολιτικούς κεντρικούς υπολογιστές, τα επεξεργάζονται, και παρέχουν τις σωστές πολιτικές πληροφορίες στον αιτούντα βασισμένο στους κανόνες ελέγχου αιτήματος και πρόσβασης. Οι κεντρικοί υπολογιστές διατηρούν επίσης τις βάσεις δεδομένων SPS με τη φόρτωση των τοπικών και μη-τοπικών πολιτικών πληροφοριών που παραλαμβάνονται μέσω των ανταλλαγών SPS. Οι πολιτικοί πελάτες παράγουν τα αιτήματα για τις πολιτικές πληροφορίες και μετασχηματίζουν τις απαντήσεις στο κατάλληλο σχήμα που απαιτείται από την εφαρμογή χρησιμοποιώντας SPS.

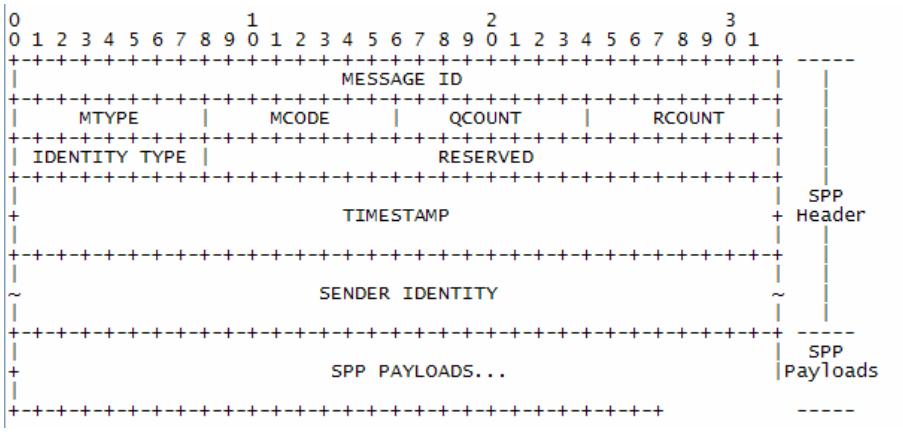


Σχήμα 1. Security Policy System

4.1.2. Security Policy Protocol

Πολιτικοί πελάτες και κεντρικοί υπολογιστές ανταλλάζουν πληροφορίες χρησιμοποιώντας το πολιτικό πρωτόκολλο ασφάλειας. Το πρωτόκολλο καθορίζει πώς οι πολιτικές πληροφορίες ανταλλάσσονται, υποβάλλονται σε επεξεργασία, και προστατεύονται από τους πελάτες και τους κεντρικούς υπολογιστές. Το πρωτόκολλο καθορίζει επίσης τι οι πολιτικές πληροφορίες είναι ανταλλαγμένος και το σχήμα χρησιμοποιημένος για να κωδικοποιήσει τις πληροφορίες. Το πρωτόκολλο έξι διαφορετικούς τύπους μηνυμάτων που χρησιμοποιούνται διευκρινίζει για να ανταλλάξουν τις πολιτικές πληροφορίες. Ένα μήνυμα SSP περιέχει ένα τμήμα επιγραφών μηνυμάτων που ακολουθείται από κανένα ή περισσότερα ωφέλιμα φορτία SSP, ανάλογα με τον τύπο μηνυμάτων.

Το σχήμα 2 απεικονίζει τη μορφή ενός μηνύματος SSP. Το τμήμα επιγραφών είναι παρόν σε κάθε μήνυμα. Περιέχει τους τομείς που προσδιορίζουν το μήνυμα, τον τύπο μηνύματος, τη θέση του μηνύματος, τον αριθμό ερωτήσεων ή/και ωφέλιμων φορτίων αρχείων, και τον οικοδεσπότη που ζητά τις πολιτικές πληροφορίες. Η επιγραφή περιλαμβάνει επίσης έναν timestamp τομέα που παρέχει την προστασία anti-replay. Μετά από την επιγραφή να υπάρξουν μηά ή περισσότερα ωφέλιμα φορτία SSP. Αυτήν την περίοδο, υπάρχουν τρεις τύποι ωφέλιμων φορτίων που καθορίζονται στα SSP: Ερώτηση, αρχείο, και ωφέλιμα φορτία υπογραφών.



Σχήμα 2. Μορφή μηνύματος SPP

Τα SSP έχουν έξι ευδιάκριτους τύπους μηνυμάτων:

- **Τα μηνύματα ερώτησης** [Query Messages] περιέχουν μια ιδιαίτερη αίτηση για τις πολιτικές πληροφορίες.
- **Τα μηνύματα απάντησης** [Reply Messages] περιλαμβάνουν τα πολιτικά αρχεία που απαντούν στις συγκεκριμένες πολιτικές ερωτήσεις.
- **Τα πολιτικά μηνύματα** [Policy Messages] περιλαμβάνουν τις πολιτικές πληροφορίες και χρησιμοποιούνται για την μεταφορά των πολιτικών ασφάλειας σε και από έναν πολιτικό κεντρικό υπολογιστή.
- **Τα μηνύματα πολιτικής αναγνώρισης** [Policy Acknowledgment Messages] χρησιμοποιούνται για να αναγνωρίσουν τα αντίστοιχα πολιτικά μηνύματα αλλά οι ίδιοι δεν περιέχουν τις πολιτικές πληροφορίες.
- **Μηνύματα μεταφοράς** [Transfer Messages], τα οποία περιέχουν τις πολιτικές πληροφορίες, χρησιμοποιούνται από τους πολιτικούς κεντρικούς υπολογιστές για να ανταλλάξουν τις μαζικές πολιτικές πληροφορίες μεταξύ των κεντρικών υπολογιστών.
- Τέλος, οι πολιτικοί κεντρικοί υπολογιστές χρησιμοποιούν **keep-alive μηνύματα** για να ενημερώσουν τις πύλες ασφάλειας και άλλες συσκευές ελέγχου για τη θέση του κεντρικού υπολογιστή.

4.1.2.1. Επικύρωση SPP μηνυμάτων

Τα μηνύματα SSP να επικυρωθούν είτε χρησιμοποιώντας IPSec είτε έναν άλλο μηχανισμό ασφάλειας. Τα SSP παρέχουν έναν βασικό μηχανισμό ασφάλειας που μπορεί να χρησιμοποιηθεί για να παρέχει την επικύρωση και την ακεραιότητα στα μηνύματά του, ειδικά όταν διαπερνά ετερογενείς περιοχές και η ταυτότητα του πολιτικού κεντρικού υπολογιστή για τον οποίο προορίζεται επιτακτικού για τον προορισμό είναι άγνωστο. Αυτές οι υπηρεσίες παρέχονται χρησιμοποιώντας τις ψηφιακές υπογραφές.

4.2. Security Policy Specification Language (SPSL)

Επίσης η Internet Engineering Task Force [IETF] καθόρισε την γλώσσα πολιτικών προδιαγραφών ασφάλειας Security Policy Specification Language [SPSL]. Είναι μια γλώσσα που δημιουργήθηκε με σκοπό να εκφράσει τις πολιτικές ασφαλείας, τις περιοχές ασφαλείας και τις οντότητες που διαχειρίζονται τις πολιτικές και τις περιοχές. Είναι μια ανεξάρτητη γλώσσα προμηθευτών και πλατφορμών για τη διευκρίνιση των πολιτικών ασφάλειας επικοινωνίας, ειδικά εκείνων που κάνουν χρήση των πρωτοκόλλων IPsec και IKE. Δεδομένου ότι η χρήση των αντιπυρικών ζωνών με την ισχυρή επικύρωση και τα ιδεατά ιδιωτικά δίκτυα (VPNs) με την κρυπτογράφηση 2 και 3 επιπέδων γίνονται δημοφιλέστερες, η ανάγκη να ρυθμιστούν αυτές οι υπηρεσίες και συσκευές ασφάλειας με τη βοήθεια των πολιτικών ασφάλειας γίνεται πιο αισθητή. SPSL επιτρέπει τις πολιτικές ασφάλειας που διευκρινίζονται σε μια διαλειτουργική γλώσσα, να αποθηκεύονται στις κοινές βάσεις δεδομένων και να υποβάλλονται σε επεξεργασία από τα συστήματα διαχείρισης χωριστά από τις συσκευές ασφάλειας.

Αν και η γλώσσα σχεδιάστηκε αρχικά για τη διευκρίνιση των πολιτικών IPsec και IKE, ο σχεδιασμό της επιτρέπει να εκφράσει τους άνευ υπηκοότητος και stateful κανόνες φιλτραρίσματος πακέτων. Επιπλέον, η γλώσσα είναι έκτακτη: οι νέες κατηγορίες αντικειμένου μπορούν να προστεθούν με σκοπό τη διευκρίνιση των πολιτικών άλλων πρωτοκόλλων ασφάλειας επικοινωνίας.

4.2.1. Απαιτήσεις SPSL

Το SPSL έχει ως σκοπό να καλύψει τις ακόλουθες απαιτήσεις:
* Υποστήριξη για IPsec/IKE και τη γενική προδιαγραφή ασφάλειας επικοινωνίας πολιτική,
* Υποστήριξη και για τον κόμβο - και περιοχή-βασισμένα πολιτικής πρότυπα,
* Υποστήριξη για τα πολλαπλάσια διανεμημένα σημεία πολιτικής επιβολής,
* Υποστήριξη για τους μηχανισμούς επικύρωσης και έγκρισης για να βοηθήσουν την πολιτική διαχείριση,
* Υποστήριξη για την ευελιξία και το επεκτασιμότητας της γλώσσας.

4.2.1.1. Node-based και Domain-Based πρότυπα

Στο SPSL υπάρχουν δύο τρόποι να συνδεθούν οι πολιτικές ασφάλειας με τις οντότητες δικτύων, γνωστές ως node-based και domain-based πολιτικά πρότυπα.

Α. Node based:(βασισμένο σε κόμβο)

Σε αυτό το πρότυπο οι πολιτικές ασφάλειας είναι συνδεδεμένες στους μεμονωμένους κόμβους δικτύων και τις συσκευές ασφάλειας (firewalls, τους οικοδεσπότες κ.λπ) Οι πολιτικές που συνδέονται με έναν κόμβο δικτύων διευκρινίζουν την προστασία για τις επικοινωνίες προς και από τον κόμβο. Αυτές οι πολιτικές αναμένονται να επιβληθούν από τον ίδιο τον κόμβο. Οι πολιτικές που συνδέονται με μια η συσκευή ασφάλειας (τυπικά γνωστή ως σημείο πολιτικής επιβολής) διευκρινίζει την προστασία για τις επικοινωνίες που περνούν μέσω αυτών των πρακτόρων. Είτε η πηγή είτε ο προορισμός της επικοινωνίας πρέπει να είναι μεταξύ των κόμβων ότι ο πράκτορας είναι εξουσιοδοτημένος να προστατεύσει. Σε αυτό το πρότυπο, και οι κόμβοι δικτύων και οι πράκτορες πολιτικής επιβολής ασφάλειας διαχειρίζονται τις πολιτικές τους.

B. Domain based:(βασισμένο σε περιοχή)

Σε αυτό το πρότυπο οι πολιτικές ασφάλειας είναι συνδεδεμένες σε μια περιοχή ασφάλειας. Μια περιοχή ασφάλειας ορίζεται ως ένα συνδεδεμένο σύνολο οντοτήτων δικτύων που προστατεύονται από τα σημεία πολιτικής επιβολής (PEP) που τοποθετούνται σε κάθε πορεία επικοινωνίας που περνά από την περίμετρο της περιοχής. Κάθε σημείο πολιτικής επιβολής της περιοχής λειτουργεί για να επιβάλει το κοινό σύνολο πολιτικών ασφάλειας που συνδέονται με την περιοχή. Οι περιοχές ασφάλειας μπορούν να είναι χωρίζουν εντελώς, στο ένα άλλη, που αποτελείται από διάφορα υποδίκτυα, ή ακριβώς τους οικοδεσπότες που επιβάλλουν την πολιτική τους. Σε αυτό το πρότυπο, οι πολιτικές που συνδέονται με μια περιοχή ρυθμίζονται από έναν ή περισσότερους ειδικούς πράκτορες κοινούς για την ολόκληρη περιοχή. Αυτοί οι ειδικοί πράκτορες ενεργούν ως πολιτικοί κεντρικοί υπολογιστές. Μπορούν να είναι ευδιάκριτες οντότητες δικτύων ή πράκτορες πολιτικής επιβολής της περιοχής.

4.2.2. Πολλαπλά διανεμημένα σημεία πολιτικής επιβολής

Το SPSL επιτρέπει τη επιλογή των σημείων επιβολής μιας πολιτικής ασφάλειας. Οι επιλογές μπορούν να είναι διεπαφές (interfaces) των κόμβων ή των πυλών ασφάλειας (firewalls) που διευκρινίζονται από τις διευθύνσεις IP. Η επιλογή ενός πράκτορα επιβολής επιτρέπει σε ένα σύστημα να επιλέξει μια πορεία επικοινωνίας διαφορετική από αυτή που επιλέγεται από τη υποδομή δρομολόγησης. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για την καθιέρωση και τη διαχείριση σηράγγων.

4.2.3. Μηχανισμοί επικύρωσης και έγκρισης

Το SPSL υποστηρίζει τις ακόλουθες υπηρεσίες ασφάλειας:

1. Ακεραιότητα στοιχείων, επικύρωση προέλευσης στοιχείων: κάθε πολιτικό αντικείμενο προστατεύεται χρησιμοποιώντας μια δημόσια υπογραφή κλειδιού. Οι αλγόριθμοι υπογραφών RSA και DSA υποστηρίζονται.

2. Επικύρωση και έγκριση των οντοτήτων πολιτικής διαχείρισης: τα διοικητικά αντικείμενα όπως maintainers συνδέουν τα δημόσια βασικά πιστοποιητικά με τους χρήστες για να επιτρέψουν την επικύρωση των πολιτικών που διανέμουν ή/και προσδιορίζονται σε ένα σύστημα διαχείρισης ασφάλειας για λόγους ελέγχου πρόσβασης.Με αυτές τις υπηρεσίες, οι χρήστες των πολιτικών SPSL προδιαγραφών μπορούν πάντα να ελέγξουν την ακεραιότητα και την προέλευση των πολιτικών και να επιτρέψουν μόνο στο εξουσιοδοτημένο προσωπικό για να διατηρήσουν τις πολιτικές.

4.2.4. Ευελιξία και επεκτασιμότητα

Η γλώσσα είναι ευέλικτη επειδή η παρούσα σύνταξή της επιτρέπει να διευκρινίσει τις πολιτικές για τις διαφορετικές χρήσεις. Παραδείγματος χάριν, μπορεί να χρησιμοποιηθεί για να διευκρινίσει τους μη-κρυπτογραφικούς κανόνες φιλτραρίσματος πακέτων καθώς επίσης και τις σήραγγες IPsec για τα εικονικά ιδιωτικά δίκτυα. Επιπλέον, υποστηρίζει και το node-based και το domain-based πρότυπο.
Η γλώσσα είναι επίσης επεκτάσιμη. Επιτρέπει νέες κατηγορίες αντικειμένου να δημιουργηθούν με την ακολουθία ενός συντακτικού κανόνα παρόμοιου με την κληρονομιά. Συνεπώς, η γλώσσα μπορεί να επεκταθεί για τη διευκρίνιση των πολιτικών της,

5. Quality of Service (ποιότητα υπηρεσιών)

5.1 Quality of Service-Εγγυήσεις

Τα εικονικά ιδιωτικά δίκτυα εκτός από την εξασφάλιση της ιδιωτικής επικοινωνίας, οι υπάρχουσες ιδιωτικές τεχνικές δικτύωσης χτισμένες πάνω σε μηχανισμούς φυσικού στρώματος ή στρώματος συνδέσεων προσφέρουν επίσης τους διάφορους τύπους ποιοτήτων των εγγυημένων υπηρεσιών. Ειδικότερα, οι μισθωμένες και dial up συνδέσεις προσφέρουν και τις εγγυήσεις εύρους ζώνης και λανθάνουσας κατάστασης, ενώ οι τεχνολογίες όπως ATM, Frame Relay έχουν τους μηχανισμούς που απαιτούνται για τις ίδιες εγγυήσεις. Δεδομένου ότι τα IP-VPNs γίνονται ευρύτερα επεκταμένα, θα υπάρξει ζήτηση στην αγορά για τις παρόμοιες εγγυήσεις, προκειμένου να εξασφαλιστεί τελείως για να τελειώσει τη διαφάνεια εφαρμογής. Ενώ η δυνατότητα βασισμένου στην IP VPNs να προσφερθούν τέτοιες εγγυήσεις θα εξαρτηθεί πολύ από τις ισόμετρες ικανότητες των ελλοχευουσών σπονδυλικών στηλών IP, ένα πλαίσιοVPN πρέπει επίσης να εξετάσει τα μέσα με τα οποία τα συστήματα VPN μπορούν να χρησιμοποιήσουν τέτοιες ικανότητες, καθώς εξελίσσονται.

5.2. Differentiated Services (διαφοροποιημένες υπηρεσίες)

Οι διαφοροποιημένες υπηρεσίες έχουν γίνει πρόσφατα η συνιστώμενη μέθοδος για να αντιμετωπίσουν τα ζητήματα Qos στα δίκτυα IP. Στο δίκτυο DiffServ τα πακέτα είναι ταξινομημένα πριν από την είσοδο του δικτύου μέσω ενός μηχανισμού χαρακτηρισμού πακέτου και η υπηρεσία που ένας δρομολογητής μέσα στο δίκτυο παρέχει σε ένα πακέτο εξαρτάται μόνο από την κατηγορία του πακέτου. Οι πληροφορίες QoS φέρονται στη ζώνη μέσα στο πακέτο στον τομέα τύπο υπηρεσιών ToS (Type of Service) της επιγραφής IP. Μια end-to-end υπηρεσία λαμβάνεται από την αλληλουχία των υπηρεσιών ανά-περιοχή και από τη συμφωνία επιπέδων υπηρεσιών SLA μεταξύ των γειτονικών περιοχών κατά

μήκος της πορείας που η κυκλοφορία διασχίζει στη μετάβαση από την πηγή στον προορισμό. Ανά περιοχή οι υπηρεσίες πραγματοποιούνται από τη βελτίωση κυκλοφορίας στην άκρη και από τους απλούς διαφοροποιημένους μηχανισμούς αποστολής στον πυρήνα του δικτύου.

Για να λάβουν τις διαφοροποιημένες υπηρεσίες από το φορέα παροχής υπηρεσιών Διαδικτύου ISP (Internet Service Provider) οι πελάτες πρέπει να έχουν μια SLA με το ISP του. Ένα SLA διευκρινίζει βασικά τις κατηγορίες υπηρεσιών που υποστηρίζονται και το ποσό κυκλοφορίας που επιτρέπεται σε κάθε κατηγορία. Ένα SLA μπορεί να είναι στατικό (Static) ή δυναμικό (Dynamic): το στατικό SLA διαπραγματεύεται σε κανονική βάση όπως μηνιαία ή ετήσια, το δυναμικό SLA πρέπει να συζητηθεί χρησιμοποιώντας πρωτόκολλο σηματοδότησης όπως είναι το RSVP για να ζητήσει τις υπηρεσίες μετά από την απαίτηση. Στη διανομή των πόρων Διαδικτύου ο έλεγχος των πόρων μπορεί να γίνει ανεξάρτητα ή μπορεί να γίνει από τους πράκτορες που έχουν κάποια γνώση των προτεραιοτήτων της οργάνωσης και των πολιτικών που πρέπει να ακολουθούνται και διαθέτει τον πόρο σεβόμενος τις πολιτικές αυτές. Αυτός ο πράκτορας αποκαλούμενος μεσίτες εύρους ζώνης BB (Bandwidth Brokers) έχει δύο ευθύνες : μια είναι να διαμοιραστούν έξω οι χαρακτηρισμένες κατανομές κυκλοφορίας της περιοχής τους και να ιδρυθούν οι δρομολογητές φύλλων μέσα στην τοπική περιοχή, άλλη μια είναι να διαχειρίζονται τα μηνύματα που στέλνονται στα όρια σε BBs των παρακείμενων περιοχών.

6. VPN Attacks

Σε αυτή την ενότητα θα ασχοληθούμε με διάφορες επιθέσεις τις οποίες μπορεί να δεχθεί ένα VPN. Για κάθε είδους επίθεση που δέχεται ένα VPN πρέπει να διευκρινίσουμε πότε είναι εξωτερική επίθεση και πότε είναι επίθεση που προήλθε από κάποια αδυναμία του VPN. Θα αναφέρουμε όλες τις δυνατές περιπτώσεις που κάποιο VPN μπορεί να δεχθεί επίθεση. Καταρχήν θα ξεκινήσουμε με τα δύο βασικά πρωτόκολλα που χρησιμοποιούνται από τα VPN δηλαδή τα IPSec και PPTP και ακολούθως θα δούμε διάφορες αδυναμίες και διάφορους τρόπους με τους οποίους μπορεί κάποιο πρωτόκολλο κρυπτογραφικό να υποστεί επιθέσεις.

6.1 Internet Security (IPSec) Attacks

Όπως έχουμε αναφέρει στην προηγούμενη παράγραφο το Internet Security Protocol (IPSec) δεν είναι ένας κρυπτογραφικός αλγόριθμος ούτε και αλγόριθμος πιστοποίησης. Είναι απλά ένα πρωτόκολλο το οποίο προσφέρει την ασφάλεια που ορίζεται στο IPSec μαζί με ορισμένους περιορισμούς. Επομένως όπως και τα άλλα πρωτόκολλα ασφαλείας το IPSec μπορεί να δεχθεί επιθέσεις. Παρακάτω αναφέρουμε μερικά είδη επιθέσεων που μπορεί να δεχθεί το IPSec.

6.1.1. Επιθέσεις κατά της διαχείρισης κλειδιού

Πρόσφατα έχει παρουσιασθεί ένα πρόβλημα με τον τρόπο που το πρωτόκολλο διαχείρισης κλειδιού (IKE) διαχειρίζεται τα κρυπτογραφικά κλειδιά στο IPSec. Στις προδιαγραφές του πρωτοκόλλου διευκρινίζεται πως αυτά τα κλειδιά πρέπει να ανταλλάσσονται αλλά συνήθως αναφέρεται μόνο για την αρχή της επικοινωνίας και όχι για το τέλος της. Λόγω του ότι υπάρχει μηχανισμός λήξης στις συναλλαγές public key, έχει διαπιστωθεί ότι δεν υπάρχει interoperability μεταξύ των vendors. Επιπρόσθετα, κάτω από τις προδιαγραφές του IKE, αν

κατά την διάρκεια της επικοινωνίας κάποιο από τα άκρα της διακόψει την επικοινωνία τότε δεν υπάρχει τρόπος να αντιληφθεί ο άλλος ότι έχει γίνει διακοπή και μπορεί να συνεχίζει να στέλνει πακέτα. Δηλαδή, αν ο ένας σταθμός εξακολουθεί να στέλνει δεδομένα τότε μπορεί να παρεμβληθεί ένας άλλος σταθμός αν χρησιμοποιούνται weak κλειδιά.

6.1.2. Αδυναμίες των IPSec

Πολλά προβλήματα μπορούν να συμβούν όταν οι vendors πιέζουν για χαρακτηριστικά που απαιτούν οι πελάτες. Αυτό, οδηγεί στην ανάπτυξη των IPSec σε περιοχές που δεν είχαν προβλεφθεί στον αρχικό σχεδιασμό και έτσι υπάρχει πιθανότητα εμφάνισης άγνωστων προβλημάτων.

6.1.2.1. Πιστοποίηση πελάτη

Το IPSec δεν έχει μηχανισμό για πιστοποίηση χρηστών όπως δικαιώματα πρόσβασης, πιστοποίηση, κ.ο.κ. Λόγω του ότι αρχικά είχε σχεδιαστεί για LAN-to-LAN VPN, δεν παρέχει μηχανισμό υποστήριξης πελατών. Με σκοπό το IPSec να μπορεί να παρέχει αυτό τον μηχανισμό, έχουν γίνει τροποποιήσεις στο αρχικό πρότυπο.

6.2. Point-to-Point Tunneling Protocol Attacks

Το PPTP πρωτόκολλο είναι ένα πολύ καλό πρωτόκολλο αλλά χρειάζεται ορισμένες βελτιώσεις όπως εξάλλου όλοι οι άλλοι κρυπτογραφικοί αλγόριθμοι. Εάν ψάξουμε στο web για PPTP πρωτόκολλα και για ασφάλεια θα βρούμε πάρα πολλά άρθρα τα οποία προτείνουν διάφορες βελτιώσεις. Λόγω του ότι το IPSec είναι παρόμοιο με το PPTP έτσι και αυτό έχει παρόμοια προβλήματα όπως το ότι δεν υποστηρίζει αλγόριθμους για encryption και authentication. Αυτό αφήνεται να γίνει από άλλα πρωτόκολλα.

Παρακάτω θα δούμε διάφορες επιθέσεις που μπορούν

να δεχθεί το πρωτόκολλο PPTP.

Α. Επιθέσεις στο GRE

Τα πακέτα του GRE μπορούν να μεταφέρουν μαζί τους ένα αριθμό από την ακολουθία τους και ένα acknowledge αριθμό ενώ για την αποφυγή της συμφόρησης μπορεί να χρησιμοποιηθεί τμηματοποιημένο παράθυρο χρόνου. Όμως αν κάποιος αποσυγχρονίσει την ακολουθία των πακέτων, τότε μπορεί να εξαπατήσει το GRE. Επίσης, το GRE δεν έχει τρόπο να αντιδράσει σε κακή ή διπλή ακολουθία αριθμών. Αυτό πιθανότατα να αγνοηθεί αλλά τότε τα πακέτα PPP μπορούν να αλλοιωθούν.

Β. Επιθέσεις κατά των passwords

Το μειονέκτημα του PPTP είναι ότι βασίζεται στο PPP και πριν από κάθε επικοινωνία το κάνει εγκατάσταση και αρχικοποιεί τις παραμέτρους επικοινωνίας. Όμως αφού το PPP δεν έχει μηχανισμό πιστοποίησης κατά τη διάρκεια της μετάδοσης αυτών των PPP πακέτων μπορεί κάποιος ενδιάμεσος να εξαπατήσει το σύστημα και να πάρει πληροφορίες για τον DNS server.

6.3. Οργανισμοί για την ασφάλεια

6.3.1. NSA (National Security Agency)

Η NSA είναι η επίσημη υπηρεσία για την ασφάλεια της κυβέρνησης των Η.Π.Α. Ο πρόεδρος Harry Truman ίδρυσε την υπηρεσία αυτή το 1952 κάτω από την επίβλεψη του υπουργείου Άμυνας της χώρας, και για πολλά χρόνια η ύπαρξή της κρατιόταν μυστική. Η NSA ασχολείται γενικά με την πληροφορία. Το έργο της είναι να παρακολουθεί και να αποκωδικοποιεί όλες τις ξένες

επικοινωνίες που αφορούν την ασφάλεια των Ηνωμένων Πολιτειών.

Η NSA διεξάγει έρευνες στην κρυπτολογία, και στον σχεδιασμό ασφαλών αλγορίθμων για την προστασία των αμερικάνικων επικοινωνιών αλλά και στον σχεδιασμό κρυπταναλυτικών τεχνικών για την παρακολούθηση των μη-αμερικανικών επικοινωνιών. Η NSA θεωρείται ως ο πιο μεγάλος εργοδότης των μαθηματικών του κόσμου, και επίσης είναι ο μεγαλύτερος αγοραστής υπολογιστικού hardware στον κόσμο. Η NSA πιθανόν κατέχει κρυπτογραφική πείρα πολλά χρόνια μπροστά από το κοινό υψηλότερο επίπεδο επιστήμης στους αλγορίθμους και μπορεί να σπάσει τα περισσότερα συστήματα που χρησιμοποιούνται στην πράξη. Αλλά, για λόγους εθνικής ασφάλειας, σχεδόν όλες οι πληροφορίες σχετικές με την NSA – ακόμη και ο προϋπολογισμός – είναι απόρρητες. (Φημολογείται ότι ο προϋπολογισμός της φτάνει στα $13 εκατομμύρια το χρόνο και είναι εργοδότης 16,000 ανθρώπων).

Η NSA χρησιμοποιεί την εξουσία της για να περιορίζει τη διαθεσιμότητα της κρυπτογραφίας στο κοινό, αυτό γίνεται για να προλάβει τους εχθρούς από την χρησιμοποίηση πολύ δυνατών κρυπτογραφικών μεθόδων που θα είναι αδύνατο η NSA να σπάσει.

6.3.2. NIST (National Institute of Standards and Technology)

Το NIST είναι ένα παράρτημα του υπουργείου Εμπορίου των Η.Π.Α. Πρώτα ονομαζόταν NBS (National Bureau of Standards) αλλά άλλαξε το όνομά του το 1988. Μέσω του Computer Systems Laboratory (CSL) το NIST προωθεί ανοιχτά πρότυπα και ελπίζει να κεντρίσει το ενδιαφέρον για οικονομική ανάπτυξη των εταιρειών που σχετίζονται με υπολογιστές. Γι’ αυτό το σκοπό το NIST εκδίδει πρότυπα και οδηγίες και ελπίζει να υιοθετηθούν από όλα τα υπολογιστικά συστήματα των ΗΠΑ. Τα επίσημα πρότυπα που δημοσιεύονται ονομάζονται FIPS (Federal Information Processing Standards) δημοσιεύσεις.

Όταν το Κογκρέσο πέρασε την πράξη για την

ασφάλεια των υπολογιστών το 1987, στο NIST δόθηκε η εντολή να ορίσει τα στάνταρτ για την εγγύηση της ασφάλειας ευαίσθητης αλλά μη απόρρητης πληροφορίας στα υπολογιστικά συστήματα της κυβέρνησης. Η πράξη εξουσιοδοτεί τη NIST με άλλες κυβερνήσεις και ιδιωτικές εταιρείες στην εκτίμηση προτεινόμενων τεχνολογικών προτύπων.

Το NIST εκδίδει πρότυπα για κρυπτογραφικές συναρτήσεις. Υπηρεσίες της κυβέρνησης των Η.Π.Α. τις χρησιμοποιούν για ευαίσθητες αλλά μη απόρρητες πληροφορίες. Συχνά και ο ιδιωτικός τομέας υιοθετεί αυτά τα πρότυπα. Το NIST έχει εκδώσει αλγόριθμους όπως ο DES, το DSS, το SHS και το EES.
Όλοι αυτοί οι αλγόριθμοι αναπτύχθηκαν με λίγη βοήθεια από την NSA που κυμαίνεται από την ανάλυση του DES μέχρι το σχεδιασμό του DSS, του SHS και τον Skipjack αλγόριθμου στο EES. Ορισμένοι έχουν κριτικάρει το NIST επειδή επιτρέπει στην NSA να έχει τόσο μεγάλο έλεγχο επάνω σ' αυτά τα πρότυπα, εφ' όσον τα ενδιαφέροντα της NSA και του NIST δεν είναι τα ίδια ακριβώς. Δεν είναι ξεκάθαρο πόσο πολύ επιρροή έχει η NSA πάνω στο σχεδιασμό και στην υλοποίηση των αλγορίθμων. Δεδομένου το περιορισμένο προσωπικό, προϋπολογισμό και πόρους του NIST, η συμμετοχή της NSA είναι αρκετά αξιοσημείωτη.

6.3.3. CERT â /CC

Το CERT/CC είναι ένα κέντρο αρμόδιο για τη συλλογή και αξιοποίηση πληροφοριών σχετικά με περιστατικά επιθέσεων στο Διαδίκτυο. Ιδρύθηκε το Νοέμβριο του 1988 και εδρεύει στο Ινστιτούτο Τεχνολογίας Λογισμικού (SEI) του Πανεπιστημίου Carnegie Mellon.

Η αφορμή για την επίσημη σύσταση του CERT®/CC ήταν η σύγχυση που προκλήθηκε το 1988, όταν ένας φοιτητής δημιούργησε και διέσπειρε στο Διαδίκτυο ένα αυτοαναπαραγόμενο πρόγραμμα βασιζόμενο στις αδυναμίες του UNIX, το Internet Worm. Μια ομάδα από ειδικούς αντιμετώπισε επιτυχώς το πρόβλημα και στη συνέχεια, κατόπιν υποδείξεως του αρμοδίου του τμήματος του Υπουργείου Άμυνας των Η.Π.Α. (DARPA)

συνέστησε το CERT®/CC, μια ομάδα για να εξασφαλίζει την ασφάλεια στο διαδίκτυο.

Το CERT®/CC πρόκειται για ένα καλά οργανωμένο ινστιτούτο ασφάλειας στο Διαδίκτυο που παρέχει ενημέρωση, τεχνική υποστήριξη και κάλυψη γενικότερα σε χρήστες του Διαδικτύου. Διαθέτει βάσεις δεδομένων με τα περισσότερα περιστατικά επιθέσεων στο Διαδίκτυο, ομάδες εκπαίδευσης και ανάπτυξης λογισμικού και γενικότερα τεχνικών θωράκισης του διαδικτύου και των δικτύων γενικότερα.

Υπάρχουν και άλλου οργανισμοί και ινστιτούτα όπως το CERT®/CC, μικρότερης εμβέλειας. Στο σύνολό τους αποτελούν το FIRST (Forum of Incident Response and Security Teams), μια μορφή κοινότητας που παρακολουθεί και επινοεί τρόπους άμυνας απέναντι σε επιθέσεις στο Διαδίκτυο. Το FIRST αριθμούσε το 1996, 57 μέλη με δράση στον κυβερνητικό, εμπορικό και ακαδημαϊκό τομέα και με σημαντική συμβολή στην ασφάλεια του αδικτύου.

7. ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Στο κεφάλαιο αυτό αναφερθήκαμε εκτενώς στην ασφάλεια και στα πρωτόκολλα πού βοηθούν για να εφαρμοστεί αυτή στα vpn δίκτυα.Όπως γίνεται κατανοητό η ασφάλεια στα δίκτυα είναι πολύ σημαντικό συστατικό για την σωστή λειτουργία τους και αυτή που θα δώσει την λεγόμενη ποιότητα υπηρεσιών.Καθώς προστατεύει τα δίκτυα από τις διάφορες επιθέσεις και κινδύνους και κατ'επέκταση και τις επιχειρήσεις.

8. ΕΠΙΛΟΓΟΣ

Συνοψίζοντας, στη σημερινή εποχή της διεθνούς διαδικτύωσης, η ασφάλεια αποτελεί μείζον θέμα για κάθε επιχείρηση που σέβεται τον εαυτό της. Είναι πλέον καθημερινό φαινόμενο η εισβολή επιτιθέμενων στα υπολογιστικά συστήματα ενός οργανισμού, και η καταστροφή και τροποποίηση ευαίσθητων δεδομένων. Επιπλέον, επιθέσεις με ιούς (viruses), hacking, cracking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service) έχουν πλέον γίνει συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπισή τους. Καθώς οι επιχειρήσεις βασίζονται όλο και περισσότερο στα εικονικά ιδιωτικά δίκτυα(VPN), οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων. Η διασύνδεση ιδιωτικών και δημόσιων δικτύων και ο διαμοιρασμός πόρων δυσκολεύει ακόμη περισσότερο τον έλεγχο της πρόσβασης σε ένα σύστημα.Όλα αυτά τα γεγονότα έχουν κάνει πολύ σημαντική την έννοια της ασφάλειας, και ουσιαστικά καθένας οφείλει να τη λάβει σοβαρά υπόψη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Tanenbaum, Andrew S. «Δίκτυα Υπολογιστών», Παπασωτηρίου 2000 (Τρίτη Έκδοση).

2. Carlo Fonda and Fulvio Postogna, COMPUTER NETWORKING BASICS,

3. William Stallings, Data and Computer Communications, Sixth edition

4. Andrew S. Tanenbaum, Computer Networks, Fourth edition

5. A GUIDE TO VIRTUAL PRIVATE NETWORKS

6. By Martin W.Murhammer , Tim A.Bourne , Tamas Gaidosch , Charles Kunzinger , Laura Rademacher , Andreas Weinfurter----------PRENTICE HALL © 1

7. IMPLEMENTING VIRTUAL PRIVATE NETWORKS

8. By Steven Brown ----------McGRAW-HILL SERIES © 1999

9. pdf file by Cisco " How Vpn Works"

10. The VPN Consortium(VPNC) web site-----VPN Technologies

11. Θεολόγου, Μ.Ε., «Δίκτυα Κινητών και Προσωπικών Επικοινωνιών», Εκδόσεις Ε.Μ.Π., 2002

12. Tanenbaum, Andrew S., «Δίκτυα Υπολογιστών», Παπασωτηρίου, 2000

13. Fred Simonds, 1996. Network Security Data and Voice Communications. McGraw-Hill.

14. Κομνηνός Θόδωρος, Σπυράκης Παύλος, 2002. Ασφάλεια δικτύων και υπολογιστικών συστημάτων. Ελληνικά Γράμματα

15. Andrew S. Tanenbaum, 2003, Fourth Edition. Computer Networks. Prentice Hall.

ΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

1. http://www.wlana.com/
2. http://news.wirelessdesignonline.com/wlan-beat/
3. Security Issues for Enterprise VPNs, white paper, http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/sevpn_wp.htm
4. Managing Virtual Private Networks-An Introduction to VPNs, white paper, http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/mnvpn_wp.htm
5. Overview of Virtual Private Networks and Cisco Secure VPN Client, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/icover.htm
6. http://www.ietf.org/html.charters/ipsec-charter.html
7. Overview of Virtual Private Networks and Cisco Secure VPN Client, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/icover.htm
8. www.techweb.com -Site με πληροφορίες, άρθρα ,links κ.λ.π.για τεχνικά θέματα σε υπολογιστές ,Δίκτυα,Internet κ.α.
9. Firewalls FAQ: http://www.interhack.net/pubs/fwfaq/