τμήμα μηχανικών πληροφορικής τ.ε.
Τ.Ε.Ι. Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ (VPN)

ΓΚΟΛΦΟΠΟΥΛΟΣ ΙΩΑΝΝΗΣ **ΧΑΛΚΙΟΠΟΥΛΟΣ ΧΡΗΣΤΟΣ**

ΑΜ : 1356 **ΑΜ : 1611**

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΤΣΑΚΑΝΙΚΑΣ ΒΑΣΙΛΕΙΟΣ

ΑΝΤΙΡΡΙΟ, ΦΕΒΡΟΥΑΡΙΟΣ 2017

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Εισαγωγή

Η παρούσα εργασία πρόκειται να ασχοληθεί με την ασφάλεια των εικονικών δικτύων, πώς έχει η σημερινή κατάσταση και ποιες είναι οι μελλοντικές εξελίξεις. Η εργασία θα ολοκληρωθεί μέσα από τέσσερα κεφάλαια, όπου πιο συγκεκριμένα, το πρώτο κεφάλαιο θα αναφερθεί αρχικά στην έννοια και τη σημασία των εικονικών δικτύων vpn και πού αυτά εφαρμόζονται.

Θα γίνει ιστορική αναδρομή για τις αρχιτεκτονικές των συστημάτων, οι λόγοι χρήσης, πού χρειάζονται και ποιες είναι οι εφαρμογές τους όπως για παράδειγμα η διαδικτυακή πρόσβαση.

Στη συνέχεια, θα αναφερθούν τα πρώτα ιδιωτικά δίκτυα, το πρωτόκολλο ip, η τεχνολογία mlps και οι αρχιτεκτονικές των εικονικών ιδιωτικών δικτύων. Έπειτα θα γίνει λόγος για τον εικονικό κόσμο , την αρχιτεκτονική δικτύων και τη δομή τους.

Το δεύτερο κεφάλαιο στη συνέχεια, θα εμβαθύνει στην ασφάλεια των δικτύων κάνοντας αναφορά στην εξασφάλιση των ηλεκτρονικών συναλλαγών και τα μέτρα ασφαλείας. Θα δοθεί βαρύτητα στην ανάλυση των Tunneling και IPsec κάνοντας λόγο για το συσχετισμό ασφαλείας και τις υλοποιήσεις λογισμικού.

Το τρίτο κεφάλαιο θα εστιάσει στους τύπους δικτύων VPN σχετικά με απομακρυσμένη πρόσβαση , την σύνδεση μέσω ενός Intranet , τις απαιτήσεις και τις τεχνολογίες του vpn.

Έπειτα θα γίνει αναφορά στα Tunneling και τα πρωτόκολα αυτών , όπως επίσης και το PPTP Point to Point Tunneling Protocol , το L2TP Layer Two Tunneling Protocol και τα είδη τούνελ IPsec - Internet Protocol Security Tunnel , όπως και το τείχος προστασίας.

Το τέταρτο και τελευταίο κεφάλαιο θα αναλύσει τα 3 ενδεχόμενα σενάρια , ενώ η εργασία θα κλείσει με τα συμπεράσματα.

Introduction

This current project is going to deal with security on virtual networks, the current situation and the future developments. The project is going to be complete through four chapters, in particular, the first chapter will refer to, the meaning and the importance of virtual networks (VPN) and where they apply.

It is going to mention the chronology of system architecture, the use, their need and how they apply, like network access.

Next, it is going to mention private networks, the internet protocol (IP), MLPS technology and the architecture of virtual private networks. Additionally will be reported to the virtual world, the architecture and their structure.

The second chapter, will extend in depth to the network security, by referring to the safeguard of electronic transactions and the security measures. Emphasis will be given to the analysis of Tunneling and IPsec, by reason of security association and software implementation.

The third chapter will emphasize to the formula of VPN network on remote access, the connection via Intranet, the requirements and the technology of VPN.

Next, it is going to refer to Tunneling and its protocol, also the PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) and the type of tunnels IPsec - Internet Protocol Security Tunnel and the firewall.

The fourth and last chapter will analyze 3 potential scenarios while the project will sum up with the conclusions

Κεφάλαιο 1: Τι είναι τα εικονικά δίκτυα vpn και που εφαρμόζονται

VPN (virtual private network) καλείται ένα δίκτυο το οποίο απαρτίζεται από εικονική υποδομή και λειτουργεί διαδικτυακά, αποτελώντας το ίδιο επίπεδο ασφάλειας με κάθε ιδιωτικό δίκτυο. Ουσιαστικά αποτελεί μία εναλλακτική λύση της κατασκευής των WAN που υποκαθιστά τα υφιστάμενα ιδιωτικά δίκτυα τα οποία εφαρμόζουν μισθωμένες γραμμές οι οποίες ανήκουν στην εταιρία. Τα ζητούμενα των virtual private network είναι όμοια αντίστοιχα με τα WAN που καλύπτουν πολλά πρωτόκολλα μαζί (Peterson, 2007) .

1.1 Ιστορική αναδρομή – Αρχιτεκτονικές των VPNs

Τα Εικονικά Ιδιωτικά Δίκτυα καλύπτουν ένα μεγάλο τεχνολογικό επίπεδο στη σημερινή εποχή και εξελισσόμενο πεδίο και βρίσκουν εφαρμογή κατά βάση σε μεγάλες επιχειρήσεις καθώς και σε περιστατικά χρηστών οι οποίοι βρίσκονται σε μακρινές περιοχές. Τα παραδοσιακά ιδιωτικά δίκτυα στηρίζονται σε μισθωμένες γραμμές με μεγάλο κόστος. Η λύση των VPNs αφορά τη χρήση της δημόσιας υποδομής, με τα ωφελήματα που αυτό συνεπάγεται σε θέματα κοστολόγησης. Επίσης εξακολουθεί να προσφέρεται αξιόπιστο αποτέλεσμα των μισθωμένων γραμμών συλλέγοντας οφέλη, με βασικότερο το μειωμένο κόστος και την μεγαλύτερη ευελιξία στη διαχείριση (Sommestad et al, 2011).

1.1.1 Λόγοι χρήσης των vpn

Τα vpn χρησιμοποιούνται ως εναλλακτική λύση της υποδομής που παρέχουν τα WAN και που αντικαθιστούν ή επαυξάνουν τα υφιστάμενα ιδιωτικά δίκτυα που κάνουν χρήση μισθωμένων γραμμών (Peterson, 2007).

1.1.2 Που χρειάζονται τα vpn

Τα εικονικά δίκτυα εξυπηρετούν στις τηλεπικοινωνιακές συνδέσεις ενός ή περισσότερων σημείων και χρησιμοποιούν την δομή που ήδη υπάρχει σε ένα δίκτυο , όπως για παράδειγμα το ίντερνετ (Peterson, 2007).

1.1.3 Εφαρμογές των vpn (πχ. πρόσβαση στο intranet από το σπίτι)

Τα εικονικά δίκτυα έχουν εφαρμογές που βασίζονται σε τεχνολογίες ATM (Asynchronous Transfer Mode), Frame Relay ή MPLS (MultiProtocol Label Switching) και εφαρμόζονται σε μισθωμένες γραμμές, σύνδεση τηλεφωνικών κέντρων, συστημάτων ασφαλείας, μετάδοση μηνυμάτων αλλά και μετάδοση ραδιοφωνικών και τηλεοπτικών εκπομπών (Peterson, 2007).

1.2 Τα πρώτα ιδιωτικά δίκτυα

Τα πρώτα ιδιωτικά δίκτυα εμφανίστηκαν το 1960. Οι εκμισθωμένες γραμμές είναι δυνατόν να χρησιμοποιηθούν για τα εξής (Peterson, 2007):

Σύνδεση Τηλεφωνικών Κέντρων

Επικοινωνία μέσω τηλεφώνου

Χρήση fax

Μετάδοση δεδομένων

Σύνδεση με το διαδίκτυο

Σύνδεση με δημόσια ή ιδιωτικά δίκτυα

Η χρήση των μισθωμένων γραμμών χαρακτηρίζεται από σταθερή χωρητικότητα , άμεση ταχύτητα μετάδοσης μέχρι 2Mbps ανά γραμμή .

1.2.1 Πρωτόκολλο IP

Το IP είναι πρωτόκολλο το οποίο χρησιμοποιείται προκειμένου να υπάρχει διασύνδεση ηλεκτρονικών υπολογιστών που είναι δυνατόν να ανήκουν στα ίδια ή σε διαφορετικά δίκτυα. Το IP μεταδίδεται με την τεχνική των πακέτων (datagrams). Το κάθε πακέτο του IP έχει φθίνουσα πορεία στον παραλήπτη δίχως να έχει εξάρτηση από άλλα πακέτα όντας αυτόνομα εντός δικτύου (Sommestad et al, 2011).

1.2.2 Τεχνολογία MPLS

Η IETF δημιούργησε το MPLS (Multiprotocol Label Switching) και είναι πρωτόκολλο το οποίο δημιουργήθηκε για να τονώσει την απόδοση του παραδοσιακού IP παρέχοντας την ίδια στιγμή καινοτόμες διαδικτυακές υπηρεσίες με τεχνολογικά συστατικά (Susanto et al, 2011)

1.2.3 Αρχιτεκτονικές Εικονικών Ιδιωτικών Δικτύων

Τα Εικονικά Ιδιωτικά Δίκτυα ταξινομούνται ποικιλοτρόπως, σύμφωνα με την οπτική που μελετώνται. Ένα Εικονικό Ιδιωτικό Δίκτυο έχει πλήρη περιγραφή μέσα από την αντιστοίχηση σε καθορισμένο είδος και για τις ανωτέρω κατηγοριοποιήσεις (Peterson, 2007).

1.3 Εικονικός κόσμος

Ο Heudin εισάγει τους Εικονικούς Κόσμους (Virtual Worlds) ως ένα νέο πεδίο έρευνας που μελετά την πολυπλοκότητα, επιχειρώντας να συνθέσει ψηφιακά σύμπαντα σε υπολογιστές. Περιλαμβάνει τα μοντέλα απλών αφηρημένων κόσμων, όπως κυτταρικά αυτόματα σε πιο εξελιγμένα εικονικά περιβάλλοντα χρησιμοποιώντας τεχνικές Εικονικής Πραγματικότητας και Τεχνητής Ζωής (Thimm & Rasmussen, 2013)

Η Εικονική Πραγματικότητα ασχολείται με τον σχεδιασμό γραφικών χώρων με την χρήση προηγμένης τρισδιάστατης σύνθεσης εικόνων. Παράλληλα με την προβολή τρισδιάστατων χώρων, δύο άλλες σημαντικές πτυχές συμμετέχουν. Η εμβύθιση και η αλληλεπίδραση. Ο χειριστής συνήθως αναπτύσσεται μέσα στον παραγόμενο κόσμο χάρη σε ένα κοστούμι δεδομένων, μία οθόνη που στερεώνεται στο κεφάλι και γάντια δεδομένων. Η ιδέα είναι να αισθάνεται «φυσικά» παρών στον εικονικό περιβάλλον και να αλληλεπιδρά με αυτόν (Wang et al, 2000).

Η Εικονική Κοινότητα (ή Inhabited Virtual World) αποτελείται από πολλούς χρήστες (MUD). Μία λεπτομερής περιγραφή των MUD δίνεται και μέσα από μια τεράστια ποσότητα καλά δομημένων πληροφοριών και υλικό, σχετικά με τα MUD που μπορεί να βρεθεί στην ιστοσελίδα. Η συνέχιση της τάσης είχε ως αποτέλεσμα την ανάπτυξη των MOO (με την προσθήκη επιπλέον χαρακτηριστικών στα MUD), των IRC και των συστημάτων τηλεδιάσκεψης, του World Wide Web και πολλών άλλων στην δεκαετία του 1990 (Peterson, 2007).

Τέλος, οι «κατοικημένοι» δυσδιάστατοι και τρισδιάστατοι εικονικοί χώροι στον κυβερνοχώρο έχουν αυξηθεί από την συγχώνευση του καναλιών συνομιλίας με κείμενο με μία οπτική διεπαφή μέσω της οποίας οι χρήστες εκπροσωπούνται από «είδωλα» (avatar). Η Εικονική Κοινότητα επικεντρώνεται στους τρισδιάστατους κόσμους, στα τρισδιάστατα είδωλα και ουσιαστικά στην κοινωνική αλληλεπίδραση και την συνομιλία (Whitman & Mattord, 2013).

Ο ορισμός που δίνεται από τον Diehl είναι ο εξής : οι εικονικοί κόσμοι είναι μοντέλα τριών διαστάσεων που βασίζονται σε υπολογιστές και αντικείμενα με περιορισμένη αλληλεπίδραση.

Ένας εικονικός κόσμος διανέμεται εφόσον τα ενεργά μέρη του εξαπλώνονται σε διαφορετικούς υπολογιστές σε ολόκληρο το δίκτυο. Δεν είναι απαραίτητο να υπάρχει κάποιος κεντρικός υπολογιστής που να έχει πλήρη γνώση του κόσμου (Xu et al, 2014).

Παρά το γεγονός ότι οι εικονικοί κόσμοι πλέον έχουν πολλές εφαρμογές πέρα από το να είναι απλώς προϊόντα ψυχαγωγίας, το γεγονός είναι ότι ξεκίνησαν ως παιχνίδια στον υπολογιστή. Επιπλέον, ίσως λόγω των μεγάλων ποσών των χρημάτων που εμπλέκονται στην δημιουργία τους και τα εγγυημένα τεράστια μηνιαία εισοδήματα που μπορούν να δημιουργήσουν, τα ηλεκτρονικά παιχνίδια στον υπολογιστή παραμένουν στην αιχμή της ανάπτυξης εικονικών κόσμων (Peterson, 2007).

Έτσι, τα ανθρώπινα όντα που αλληλεπιδρούν με το προσομοιωμένο περιβάλλον είναι γνωστά ως *παίκτες* και όχι ως χρήστες. Τα μέσα με τα οποία το περιβάλλον παρουσιάζει τους στόχους στους παίκτες ονομάζεται *εμπειρία παιχνιδιού* και η δραστηριότητα της αλληλεπίδρασης με το περιβάλλον αναφέρεται ως *παιχνίδι*.

Οι ειδικοί μπορεί να υιοθετήσουν ένα διαφορετικό λεξιλόγιο, πιο επίσημο για τον συγκεκριμένο τομέα της ειδικότητάς τους. Για παράδειγμα ένας πολιτιστικός ανθρωπολόγος μπορεί να προτιμά να μιλά για «άτομα» που παρουσιάζουν «συμπεριφορές» ως απάντηση σε «πιέσεις». Ωστόσο, σε οποιαδήποτε ευρύτερη συζήτηση του θέματος κυριαρχεί η ορολογία που προσανατολίζεται στην έννοια του παιχνιδιού και ως εκ τούτου είναι αυτή που θα χρησιμοποιηθεί και εδώ (Yan & Ma, 2014).

Είναι σημαντικό να σημειωθεί ότι εικονικοί κόσμοι δεν είναι το ίδιο όπως η εικονική πραγματικότητα, η οποία έχει ένα πολύ πιο συγκεκριμένο νόημα. Η εικονική πραγματικότητα ασχολείται κυρίως με τους μηχανισμούς με τους οποίους τα ανθρώπινα όντα αλληλεπιδρούν με προσομοιώσεις σε υπολογιστές, δεν ασχολείται ιδιαίτερα με την φύση των ίδιων των προσομοιώσεων. Οι άνθρωποι που επισκέπτονται τους εικονικούς κόσμους μπορεί κάποια μέρα να επωφεληθούν από την τεχνολογική έρευνα (π.χ. γάντια δεδομένων), αλλά η θεμελιώδης έλξη γι' αυτούς είναι αυτό που τους περιμένει όταν εισέρχονται σε έναν εικονικό κόσμο και όχι τα μέσα με τα οποία πραγματοποιείται αυτό το πιο βασικό επίπεδο, οι εικονικοί κόσμοι είναι

αντανακλάσεις των δημιουργών τους. Ως εκ τούτου, το πρώτο θέμα που διερευνήθηκε εξετάζει τις αποφάσεις σχεδιασμού του εικονικού κόσμου των δημιουργών καθώς και τις επιπτώσεις για το συγκεκριμένο άτομο και τις συμπεριφορές των avatar υπό διαφορετικές στρατηγικές σχεδιασμού. Παρά το γεγονός ότι υιοθετούμε τον όρο των εικονικών κόσμων με μία σχετική χαλαρότητα, για να συμπεριλάβουμε όλα τα είδη της τρισδιάστατης προσομοίωσης των περιβαλλόντων με την χρήση υπολογιστή, υπάρχει μια μεγάλη ποικιλομορφία στα σχέδια των εικονικών κόσμων, τα οποία έχουν ενδιαφέρουσες επιπτώσεις στα αποτελέσματα (Zafar, 2013).

Για παράδειγμα, προηγούμενες έρευνες περιγράφουν το πώς οι εικονικοί κόσμοι μπορούν να χαρτογραφηθούν σύμφωνα με δύο βασικές διαστάσεις: μια διάσταση φαντασίας-ρεαλισμού και μία διάσταση εξέλιξης-εμφάνισης. Η διάσταση εξέλιξη- εμφάνιση δείχνει τον βαθμό στον οποίο οι δραστηριότητες στον κόσμο σχηματίζονται και υπαγορεύονται από τους δημιουργούς των κόσμων (π.χ. World of Warcraft) ή αναδύονται μέσα από τις αλληλεπιδράσεις με άλλα είδωλα (π.χ. κοινωνικοί εικονικοί κόσμοι όπως το Second Life).

Οι δημιουργοί του εικονικού κόσμου δεν πρέπει μόνο να εξετάζουν το πώς μπορούν να διαμορφώσουν τους κόσμους σε αυτές τις δύο διαστάσεις, αλλά πρέπει επίσης να προβούν σε σημαντικές αποφάσεις σχετικά με το ποιος μπορεί να δημιουργήσει αντικείμενα και πώς, ποιος είναι ο ιδιοκτήτης της πνευματικής ιδιοκτησίας που προκύπτει από τις εργασίες ή/και το σενάριο που έχει επενδυθεί και πώς ισορροπούν η λήψη αποφάσεων και ο έλεγχος μεταξύ των δημιουργών του εικονικού κόσμου και των χρηστών που τον κατοικούν. Μόλις ληφθούν αυτές οι βασικές αποφάσεις, εξακολουθεί να υπάρχει μία μεγάλη πρόκληση ως προς τον πραγματικό σχεδιασμό του πληροφοριακού συστήματος που διέπει τον εικονικό κόσμο (Furst et al., 2002).

Στο άρθρο του «The Control Over Virtual Worlds by Game Companies: Issues and Recommendations», ο Christophe Roquilly εξετάζει αυτό που αναφέρεται ως «5Cs» ή πέντε βασικοί παράγοντες που χρησιμοποιούν οι δημιουργοί κατά την ανάπτυξη και τον έλεγχο των εικονικών κόσμων τους. Οι πρώτοι τέσσερις παράγοντες σχετίζονται με τον σχεδιασμό του εικονικού κόσμου (δικαιώματα πνευματικής ιδιοκτησίας, κώδικας, δημιουργικότητα και κοινότητα) και είναι ισχυρά, αλληλένδετα συστατικά που χρησιμοποιούν οι δημιουργοί για να καθορίσουν τι είναι και τι δεν είναι δυνατόν στον εικονικό κόσμο τους.

Για παράδειγμα, όσο περισσότερο περιορίζεται ένας χρήστης από την άποψη της δημιουργικότητας, λόγω του σεναρίου του εικονικού κόσμου, τόσο περισσότερο ένας δημιουργός εικονικού κόσμου πρέπει να χρησιμοποιεί αυστηρούς κώδικες υπολογιστή που θα επιτρέπουν στους χρήστες να εκτελούν μόνο τις δράσεις που προβλέπονται στο σενάριο του εικονικού του κόσμου. Το πέμπτο C είναι ένα συμπληρωματικό στοιχείο (οι συμβάσεις) που οι δημιουργοί στην συνέχεια χρησιμοποιούν για να ενισχύσουν τον έλεγχο πάνω στους χρήστες (Peterson, 2007).

Εξετάζοντας τις συμφωνίες άδειας χρήσης τελικού χρήστη (EULA) και τους όρους της υπηρεσίας (TOS) σε 20 διαφορετικούς εικονικούς κόσμους, ο Roquilly αναπτύσσει ιδέες για το πώς οι δημιουργοί του εικονικού κόσμου προσπαθούν να δημιουργήσουν βιώσιμα επιχειρηματικά μοντέλα με τον χειρισμό των 5C για να ασκήσουν ορισμένο βαθμό ελέγχου επί των υπηρεσιών που θέτουν στην διάθεση των χρηστών. Αυτές οι ιδέες αποκαλύπτουν ότι οι εικονικοί κόσμοι δεν είναι μόνο απλά περιβάλλοντα, αλλά περίπλοκες λειτουργίες ενσωματωμένες μέσα σε μια ευημερούσα και άκρως ανταγωνιστική παγκόσμια βιομηχανία.

Για παράδειγμα, τα δικαιώματα ιδιοκτησίας γίνονται ολοένα και πιο αμφιλεγόμενα σε διεθνή κλίμακα και παραδόξως, οι συμφωνίες άδειας χρήσης τελικού χρήστη και οι όροι της υπηρεσίας από τις εξεταζόμενες εταιρείες παρουσιάζουν στην πραγματικότητα μεγαλύτερο νομικό κίνδυνο για τους δημιουργούς του εικονικού κόσμου από ό,τι παρέχουν ασφάλεια.

Στην συνέχεια παρέχονται βασικές συστάσεις για το πώς πρέπει να ευθυγραμμιστούν οι διατάξεις της σύμβασης για την υποστήριξη του επιλεγμένου επιχειρηματικού μοντέλου για την λήψη αποφάσεων που ωφελούν τόσο τους χρήστες όσο και τους δημιουργούς.

Μόλις οι δημιουργοί του εικονικού κόσμου καθιερώσουν τα 5Cs και σχεδιάσουν τις δομές τους, οι χρήστες καλούνται να κατοικήσουν τον κόσμο. Οι χρήστες στην συνέχεια έρχονται αντιμέτωποι με την σημαντική πρόκληση της κατανόησης αυτού του νέου περιβάλλοντος, μέσω της συμμετοχής και των αλληλεπιδράσεών τους με άλλα είδωλα, αντικείμενα και το ίδιο το περιβάλλον.

Σύμφωνα με τον John “Pathfinder” Λέστερ, έναν στρατηγικό παίκτη στον εικονικό κόσμο, πριν στο Second Life και τώρα στο ReactionGrid, ένας από τους σημαντικότερους λόγους για τους οποίους το hype γύρω από τους εικονικούς κόσμους δεν εξελίχθηκε σε πραγματικό κύμα καινοτομίας είναι ότι οι άνθρωποι είχαν κολλήσει στον παλιό τρόπο σκέψης και έτσι αναπαρήγαγαν εμπειρίες από τον πραγματικό κόσμο στον εικονικό κόσμο (Peterson, 2007).

1.4 Αρχιτεκτονική δικτύων.

Σε έναν σύγχρονο κόσμο που υποστηρίζεται από μεγάλα, πολύπλοκα δίκτυα, τα παραδείγματα κυμαίνονται από τις χρηματοπιστωτικές αγορές μέχρι τα συστήματα επικοινωνιών και μεταφορών. Σε πολλές περιπτώσεις η ρεαλιστική ροή των φυσικών ποσοτήτων στο δίκτυο, όπως χαρακτηρίζεται από τα φορτία στους κόμβους, είναι σημαντική. Θα αποδειχτεί ότι για τα εν λόγω δίκτυα, όπου τα φορτία μπορούν να ανακατανεμηθούν μεταξύ των κόμβων, οι εσκεμμένες επιθέσεις μπορεί να οδηγήσουν σε μια σειρά από

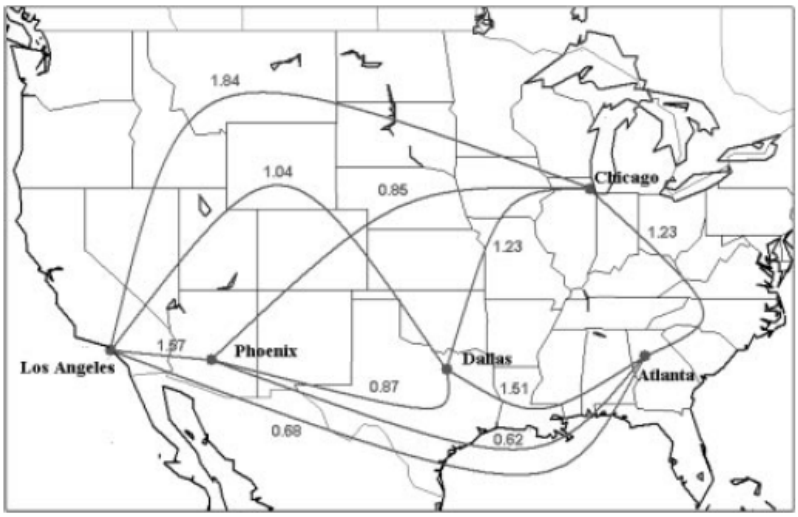
αποτυχίες υπερφόρτωσης, οι οποίες μπορούν με τη σειρά τους να προκαλέσουν την κατάρρευση του συνόλου του δικτύου ή ενός σημαντικού μέρους του. Αυτό έχει σημασία για τα δίκτυα του πραγματικού κόσμου τα οποία διαθέτουν μια πολύ ετερογενή κατανομή φορτίων, όπως το Διαδίκτυο και τα δίκτυα ηλεκτρικής ενέργειας. Φαίνεται ότι η ετερογένεια των δικτύων αυτών τα καθιστά ιδιαίτερα ευάλωτα σε επιθέσεις όπου μία μεγάλης κλίμακας αλληλεπικάλυψη μπορεί να προκληθεί από την απενεργοποίηση ενός μόνο βασικού κόμβου. Αυτό εγείρει προφανείς ανησυχίες σχετικά με την ασφάλεια των συστημάτων αυτών.

Το τριαδικό κλείσιμο όντως ασκεί μια ισχυρή επίδραση στον σχηματισμό συνδέσεων, αλλά οι συντομεύσεις με βάση την κίνηση αποτελούν έναν άλλο βασικό παράγοντα για την ερμηνεία της εξέλιξης του δικτύου. Ωστόσο, οι ατομικές στρατηγικές για την παρακολούθηση άλλων χρηστών, είναι πολύ ετερογενείς. Οι συμπεριφορές δημιουργίας συνδέσεων μπορούν να συνοψιστούν με την κατάταξη των χρηστών σε διάφορες κατηγορίες με διακριτά δομικά και συμπεριφοριστικά χαρακτηριστικά. Οι χρήστες που είναι δημοφιλείς, ενεργοί και ασκούν επιρροή τείνουν να δημιουργούν συντομεύσεις κυκλοφορίας, καθιστώντας την διαδικασία διάχυσης των πληροφοριών πιο αποτελεσματική στο δίκτυο (Dovrolis, 2013).

Τα Προσαρμοζόμενα Δίκτυα εμφανίζονται σε πολλές βιολογικές εφαρμογές. Συνδυάζουν την τοπολογική εξέλιξη του δικτύου με την δυναμική στους κόμβους του δικτύου. Πρόσφατα, η δυναμική των Προσαρμοζόμενων Δικτύων έχει διερευνηθεί σε έναν αριθμό παράλληλων μελετών από διαφορετικά πεδία, τα οποία κυμαίνονται από την Γονιδιωματική έως την Θεωρία Παιγνίων. Εδώ μελετώνται αυτές οι πρόσφατες εξελίξεις και αποδεικνύεται ότι μπορούν να μελετηθούν από μια μοναδική οπτική γωνία. Αποδεικνύεται ότι όλες αυτές οι μελέτες χαρακτηρίζονται από κοινά θέματα και κυρίως την σύνθετη δυναμική και την ισχυρή τοπολογική αυτο-οργάνωση που βασίζεται σε απλούς τοπικούς κανόνες.

Η εξέλιξη παράγει σύνθετα και δομημένα δίκτυα αλληλεπιδρώντων συστατικών στοιχείων σε χημικά, βιολογικά και κοινωνικά συστήματα. Περιγράφεται ένα απλό μαθηματικό μοντέλο για την εξέλιξη ενός ιδεατού χημικού συστήματος για να μελετηθεί ο τρόπος με τον οποίον προκύπτει και εξελίσσεται ένα δίκτυο συνεργατικών μοριακών ειδών προκειμένου να γίνει πιο περίπλοκο και δομημένο. Το δίκτυο μοντελοποιείται από ένα κατευθυνόμενο σταθμισμένο γράφημα του οποίου οι θετικές και αρνητικές συνδέσεις αναπαριστούν «καταλυτικές» και «ανασταλτικές» αλληλεπιδράσεις μεταξύ των μοριακών ειδών και το οποίο εξελίσσεται καθώς τα είδη με τους μικρότερους πληθυσμούς αντικαθίστανται από νέα. Ένα μικρό αυτοκαταλυτικό σύνολο, που εμφανίζονται κατά τύχη, παρέχει τον σπόρο για την αυθόρμητη ανάπτυξη της διασύνδεσης και συνεργασίας στο γράφημα. Προκύπτει αναπόφευκτα μία εξαιρετικά δομημένη χημική οργάνωση, καθώς το αυτοκαταλυτικό σύνολο διευρύνεται και διεισδύει μέσω του δικτύου σε ένα σύντομο χρονικό διάστημα που καθορίζεται αναλυτικά.

Αυτή η αυτοοργάνωση δεν απαιτεί την παρουσία αυτοαναπαραγόμενων ειδών. Το δίκτυο παρουσιάζει επίσης καταστροφές σε μεγάλες χρονικές κλίμακες που προκλήθηκαν από την τυχαία κατάργηση «θεμελιωδών» ειδών, τις οποίες ακολουθούν ανακάμψεις (Dovrolis, 2013). Μαζί με μια περίπλοκη τοπολογική δομή, τα πραγματικά δίκτυα εμφανίζουν μεγάλη ετερογένεια στην ικανότητα και την ένταση των συνδέσεων. Αυτά τα χαρακτηριστικά, ωστόσο, δεν έχουν ληφθεί υπόψη σε προηγούμενες μελέτες όπου οι συνδέσεις συνήθως παρουσιάζονται ως δυαδικές καταστάσεις, δηλαδή, είτε υπάρχουν ή δεν υπάρχουν. Εδώ, μελετάμε το επιστημονικό δίκτυο συνεργασίας και το παγκόσμιο δίκτυο αερομεταφορών, τα οποία είναι αντιπροσωπευτικά παραδείγματα των συστημάτων κοινωνικών και μεγάλων έργων υποδομής, αντίστοιχα (Dovrolis, 2013). Σε αμφότερες τις περιπτώσεις είναι δυνατόν να εκχωρηθεί σε κάθε ακμή του γραφήματος ένα βάρος ανάλογο προς την ένταση ή την ικανότητα των συνδέσεων μεταξύ των διαφόρων στοιχείων του δικτύου. Καθορίζονται οι κατάλληλες μετρήσεις που συνδυάζουν τα σταθμισμένα και τοπολογικά παρατηρήσιμα που θα μας επιτρέψουν να χαρακτηρίσουμε τις πολύπλοκες στατιστικές ιδιότητες και την ετερογένεια της πραγματικής δύναμης των ακμών και κορυφών. Η πληροφορία αυτή μας επιτρέπει να διερευνήσουμε τις συσχετίσεις μεταξύ των σταθμισμένων ποσοτήτων και την υποκείμενη τοπολογία του δικτύου. Αυτά τα αποτελέσματα παρέχουν μια καλύτερη περιγραφή των ιεραρχιών και των αρχών οργάνωσης στην βάση της αρχιτεκτονικής των σταθμισμένων δικτύων (Peterson, 2007).

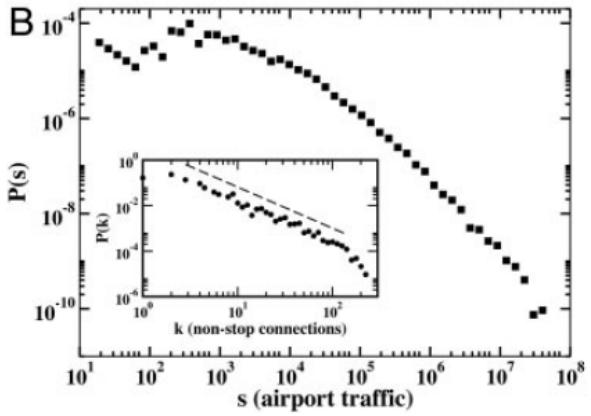


Γράφημα 1.1 αρχιτεκτονική των σταθμισμένων δικτύων.

Πηγή: Dovrolis C (2013) CS8803-NS Network Science Fall , Ανάκτηση από: http://www.cc.gatech.edu/~dovrolis/Courses/NetSci/ (30.1.2016)

Εικονική απεικόνιση του σταθμισμένου γραφήματος που λήφθηκε από τα δεδομένα του δικτύου αερολιμένων. Τα μεγάλα αεροδρόμια των ΗΠΑ συνδέονται με ακμές υποδηλώνοντας την παρουσία μίας

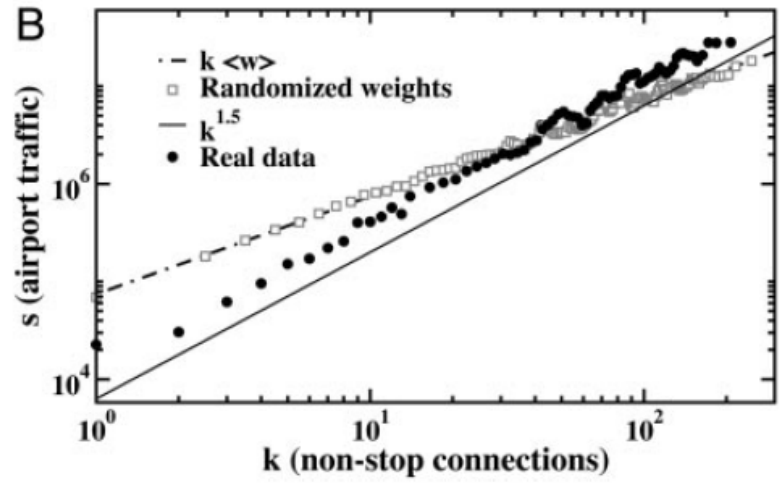
απευθείας πτήσης προς τις δύο κατευθύνσεις των οποίων τα βάρη αντιπροσωπεύουν τον αριθμό των διαθέσιμων θέσεων (εκατομμύρια/έτος).



Γράφημα 1.2 Κατανομή ισχύος

Πηγή: Dovrolis C (2013) CS8803-NS Network Science Fall , Ανάκτηση από: http://www.cc.gatech.edu/~dovrolis/Courses/NetSci/ (30.1.2016)

(Β) Οι ίδιες κατανομές για την WAN. Στην περίπτωση αυτή, η κατανομή των βαθμών μπορεί να προσεγγιστεί με βάση την συμπεριφορά του δυναμικού νόμου $P(k) \sim k^{-\gamma}$ με $\gamma = 1.8 \pm 0.2$. Η κατανομή ισχύος έχει μία βαριά υψηλή έκταση σε περισσότερες από τέσσερις τάξεις μεγέθους (Dovrolis, 2013).



Γράφημα 1.3 Σχέση μεταξύ ισχύος και βαθμού

Πηγή: Dovrolis C (2013) CS8803-NS Network Science Fall , Ανάκτηση από: http://www.cc.gatech.edu/~dovrolis/Courses/NetSci/ (30.1.2016)

(Β) Τα πραγματικά δεδομένα WAN ακολουθούν μία συμπεριφορά δυναμικού νόμου με εκθέτη $\beta = 1.5 \pm 0.1$. Η τιμή αυτή υποδηλώνει τις ανώμαλες συσχετίσεις μεταξύ της κίνησης που διαχειρίζεται ένα αεροδρόμιο και του αριθμού των δρομολογίων του.

1.5 Δομή δικτύων

Η δομή ενός δικτύου μπορεί να επηρεάσει σημαντικά τις ιδιότητες των δυναμικών διεργασιών που λαμβάνουν χώρα σε αυτά. Ενώ πολλές μελέτες έχουν ασχοληθεί με αυτήν την επίδραση, πολύ λιγότερη προσοχή έχει δοθεί στους μηχανισμούς αλληλεπίδρασης και ανατροφοδότησης μεταξύ των δυναμικών διεργασιών και την τοπολογία του δικτύου στα προσαρμοζόμενα δίκτυα. Η αναδιαμόρφωση της συνδεσμολογίας στα προσαρμοζόμενα δίκτυα μπορεί να πραγματοποιηθεί σε συστήματα στην πραγματική ζωή, όπως στα δίκτυα γνωριμιών όπου οι άνθρωποι είναι πιο πιθανό να διατηρήσουν μια κοινωνική σχέση αν οι απόψεις και οι αξίες τους είναι παρόμοιες. Μελετώνται διαφορετικές παραλλαγές ενός μοντέλου για τον σχηματισμό συναίνεσης.

Οι έρευνες δείχνουν ότι η προσαρμογή της τοπολογίας του δικτύου ενισχύει τον σχηματισμό συμπλέγματος με την ενίσχυση της επικοινωνίας μεταξύ των συντελεστών με παρόμοια άποψη, παρόλο που αυτό προωθεί, επίσης, τον καταμερισμό αυτών των συμπλεγμάτων.

Η χρονική συμπεριφορά επηρεάζεται επίσης έντονα από την προσαρμοστικότητα: ενώ, στα στατικά δίκτυα, επηρεάζεται από τις ιδιότητες της διήθησης, στα προσαρμοζόμενα δίκτυα, τόσο οι πρώιμες, όσο και οι όψιμες χρονικές εξελίξεις του συστήματος καθορίζονται από την διαδικασία της αναδιαμόρφωσης της συνδεσμολογίας. Η έρευνα μιας παραλλαγής του μοντέλου αποκαλύπτει ότι τα σενάρια των μεταβάσεων μεταξύ καταστάσεων συναίνεσης και πόλωσης είναι πιο ισχυρά στα προσαρμοζόμενα δίκτυα.

Τα πραγματικά δίκτυα συχνά εμφανίζουν και τους δύο τύπους της δυναμικής, σχηματίζοντας ένα προσαρμοστικό ή συν-εξελικτικό σύστημα στο οποίο η τοπολογία του δικτύου και η κατάσταση των κόμβων/συνδέσεων επηρεάζουν ο ένας τον άλλο σε έναν βρόχο ανάδρασης. Εδώ γίνεται εστίαση στην συν-εξελικτική δυναμική των online κοινωνικών δικτύων και ειδικότερα στο Twitter. Φαίνεται η παρουσία τέτοιας συν-εξελικτικής δυναμικής, προτείνεται ένα μοντέλο για να συλληφθεί η πιθανότητα και το χρονοδιάγραμμα πραγματοποίησής τους και συζητάται η σημασία τους ως προς την δομή και την λειτουργία του δικτύου.

Ως επί το πλείστον δίνεται βαρύτητα σε έναν τύπο συν-εξελικτικής δυναμικής στο Twitter, δηλαδή στην προσθήκη νέων συνδέσεων ακολούθων, ως αποτέλεσμα των retweets. Παρακολουθώντας την δραστηριότητα

χιλιάδων χρηστών του Twitter σχεδόν σε πραγματικό χρόνο και ιχνηλατώντας τους ακολούθους τους και τα tweets/retweets, συλλέγονται δεδομένα που επιτρέπουν την συναγωγή αυτών των νέων σχέσεων των ακολούθων που ενεργοποιούνται από τα retweet (Dovrolis, 2013).

Αποδεικνύεται ότι ο σχηματισμός αυτών των σχέσεων είναι πολύ πιο πιθανός από ό, τι η εξωγενής άφιξη νέων ακολούθων ελλείψει νέων retweets και προσδιορίζεται στους πιο σημαντικούς παράγοντες σε αυτό το φαινόμενο, δηλαδή, την αμοιβαιότητα και τον αριθμό των retweets που ένας πιθανός νέος ακόλουθος λαμβάνει σε ένα δεδομένο χρονικό διάστημα. Συζητάμε επίσης τις επιπτώσεις μιας τέτοιας συν-εξελικτικής δυναμικής στην τοπολογία και την λειτουργία ενός online κοινωνικού δικτύου. Τέλος, μελετάται εν συντομία μια δεύτερη εμφάνιση της συν-εξελικτικής δυναμικής στο Twitter, δηλαδή η πιθανότητα που ένας χρήστης αφαιρεί έναν σύνδεσμο ακολούθου αφού δέχτηκε ένα tweet ή retweet από τον αντίστοιχο ακολουθούμενο (Peterson, 2007).

Κεφάλαιο 2: Ασφάλεια δικτύων

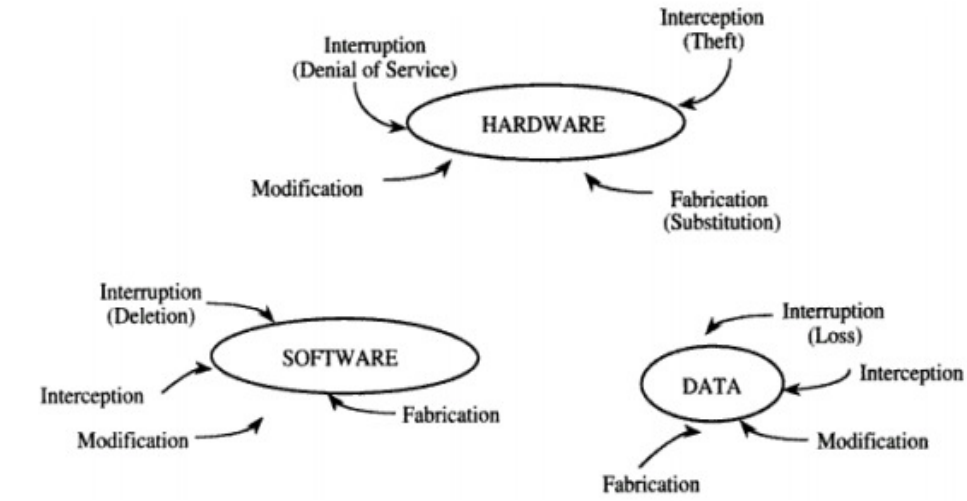
Η πολιτική ασφάλειας για τα ΠΣ μιας επιχείρησης έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να πραγματοποιηθεί με ποικίλους τρόπους, όπως χρήση προτύπων διαχείρισης σχετικά με την ασφάλεια. Στη συνέχεια δίνονται οι ορισμοί που για στην ανάλυση κινδύνων (Spears & Barki, 2010):

1. **Απειλή**: Ένα μη επιθυμητό γεγονός που μπορεί να προξενήσει μη διαθεσιμότητα του συστήματος

2. **Ευπάθεια**: Μια σχεδιαστική ατέλεια σε ένα σύστημα, με δυνατότητα παραβίασης της ασφάλειας του συστήματος.

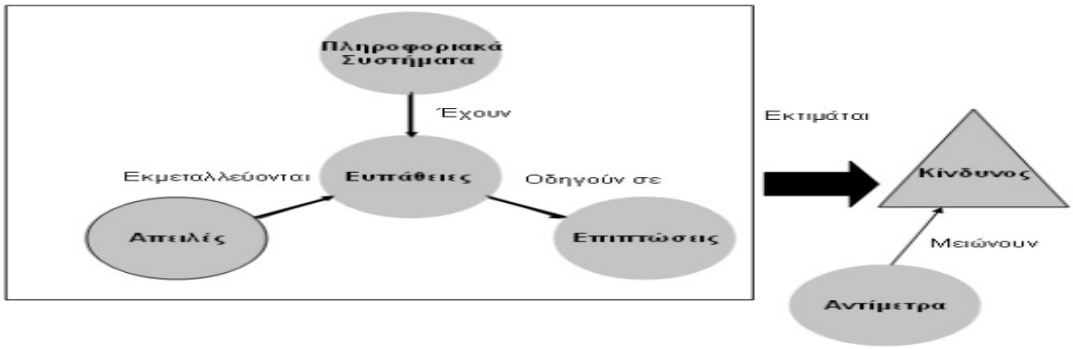
3. **Κίνδυνος**: Ενδεχόμενο κινδύνου στο να εκμεταλλευτεί μια απειλή μια ευπάθεια.

4. **Αντίμετρο**: Μέτρο που εφαρμόζεται για την προστασία του ΠΣ και την αντιμετώπιση των απειλών.



Σχήμα 2.1. Ευπάθειες ενός πληροφοριακού συστήματος

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.



Σχήμα 2.2. Συσχέτισης των παραγόντων της ανάλυσης επικινδυνότητας

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.

Η Διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της προσβασιμότητας των πληροφοριών. Επιπλέον, άλλες ιδιότητες όπως η αυθεντικότητα, η λογοδοσία, μη άρνηση και η αξιοπιστία μπορεί να συμπεριληφθούν.

Ο όρος "διαθεσιμότητα" δεν έχει χρησιμοποιηθεί σε αυτόν τον ορισμό, γιατί είναι ένας όρος που ορίζεται σε αυτό το τμήμα του ISO / IEC 20000 το οποίο δεν θα ήταν κατάλληλο για τον ορισμό αυτό .

Το Περιστατικό ασφάλειας πληροφορίας, αποτελεί ένα μεμονωμένο ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών που έχουν σημαντική πιθανότητα να θέτουν σε κίνδυνο τις επιχειρηματικές δραστηριότητες και απειλεί την ασφάλεια των πληροφοριών. Το Ενδιαφερόμενο μέρος είναι ένα άτομο ή ομάδα που έχει ένα ιδιαίτερο ενδιαφέρον για την απόδοση ή την επιτυχία της δραστηριότητας ή των δραστηριοτήτων του φορέα παροχής υπηρεσιών. Οι πελάτες, οι ιδιοκτήτες, η διαχείριση, οι άνθρωποι στην οργάνωση, οι προμηθευτές του φορέα παροχής υπηρεσιών, οι τραπεζίτες, οι συνδικαλιστικές οργανώσεις ή οι εταίροι.

Η Εσωτερική ομάδα αποτελεί μέρος της οργάνωσης του φορέα παροχής υπηρεσιών που συνάπτει τεκμηριωμένη συμφωνία με τον πάροχο υπηρεσιών να συμβάλλει στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών. Η εσωτερική ομάδα είναι εκτός του πεδίου εφαρμογής των SMS του φορέα παροχής υπηρεσιών. Ένα άλλο σημαίνον στοιχείο αποτελεί ένα γνωστό σφάλμα, το αποτελεί ένα πρόβλημα που έχει εντοπισμένη αιτία ή μια μέθοδος μείωσης ή εξάλειψης των επιπτώσεων του σε μια υπηρεσία μέσω της εργασίας γύρω από αυτό

Σημαίνον στοιχείο στην ασφάλεια των πληροφοριακών συστημάτων καθίσταται η οργάνωση η οποία

είναι μια ομάδα ανθρώπων και εγκαταστάσεων, με διάταξη των ευθυνών, των αρχών και των σχέσεων. Ένα άλλο σημαίνον στοιχείο είναι η λεγόμενη Προληπτική δράση, η οποία αποτελεί μια δράση για την αποφυγή ή την εξάλειψη των αιτίων ή τη μείωση της πιθανότητας εμφάνισης μιας πιθανής μη συμμόρφωσης ή άλλων δυνητικών ανεπιθύμητων καταστάσεων. Παρακάτω παραθέτονται επίσης σημαίνοντες ορισμοί(Γιαννόπουλος 2001):

1. Πρόβλημα: Αιτία από ένα ή περισσότερα επεισόδια. Η αιτία δεν είναι συνήθως γνωστή κατά το χρόνο καταγραφής του προβλήματος και η διαδικασία διαχείρισης των προβλημάτων είναι υπεύθυνη για την περαιτέρω έρευνα.

2. Διαδικασία: Καθορισμένος τρόπος για την πραγματοποίηση μια δραστηριότητας ή διαδικασίας

3. Διεργασία: Το σύνολο των αλληλένδετων ή αλληλεπιδρώντων δραστηριοτήτων που μετατρέπει τις εισροές σε εκροές

4. Καταγραφή: Έγγραφο που αναφέρει αποτελέσματα που επιτεύχθηκαν ή παρέχει αποδείξεις δραστηριοτήτων που πραγματοποιήθηκαν

5. Απελευθέρωση: Συλλογή ενός ή περισσοτέρων νέων ή τροποποιημένων στοιχείων διαμόρφωσης που έχουν αναπτυχθεί στο ζωντανό περιβάλλον ως αποτέλεσμα μίας ή περισσοτέρων αλλαγών

6. Αίτημα για αλλαγή: Πρόταση για μια αλλαγή που πρέπει να γίνει σε μια υπηρεσία, στοιχείο υπηρεσίας ή του συστήματος διαχείρισης των υπηρεσιών. Μια αλλαγή σε μια υπηρεσία περιλαμβάνει την παροχή μιας νέας υπηρεσίας ή την αφαίρεση μιας υπηρεσίας η οποία δεν είναι πλέον απαραίτητη .

7. Κίνδυνος: Επίδραση της αβεβαιότητας για τους στόχους. Ένα αποτέλεσμα είναι μια απόκλιση από την αναμενόμενη - θετική ή / και αρνητική. Οι στόχοι μπορούν να έχουν διαφορετικές πτυχές (όπως οικονομικούς στόχους, την υγεία και την ασφάλεια, και περιβαλλοντικούς στόχους) και μπορεί να εφαρμοστεί σε διαφορετικά επίπεδα (όπως στρατηγικά, σε ολόκληρο τον οργανισμό, το έργο, το προϊόν και τη διαδικασία) .

8. Υπηρεσία: Μέσο για την παροχή αξίας στον πελάτη, διευκολύνοντας τα αποτελέσματα που θέλει να επιτύχει ο πελάτης. Μια υπηρεσία μπορεί επίσης να παραδοθεί με τον παροχέα υπηρεσιών από έναν προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής.

9. Συνιστώσα των υπηρεσιών: Ενιαία μονάδα μιας υπηρεσίας που όταν συνδυάζεται με άλλες μονάδες θα παραδώσει μια πλήρη υπηρεσία.

10. Συνέχεια των υπηρεσιών: Δυνατότητα διαχείρισης των κινδύνων και των γεγονότων που θα μπορούσαν να έχουν σοβαρές επιπτώσεις σε μια υπηρεσία ή υπηρεσίες, προκειμένου να παραδώσει συνεχώς τις υπηρεσίες σε αποδεκτά επίπεδα

11. Σύμβαση Παροχής Υπηρεσιών: Τεκμηριωμένη σύμβαση μεταξύ του παρόχου υπηρεσιών και του πελάτη που προσδιορίζει τις υπηρεσίες και τους στόχους των υπηρεσιών. Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί επίσης να καθοριστεί μεταξύ του παρόχου υπηρεσιών και του προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής .Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί να συμπεριληφθεί σε μια σύμβαση ή άλλου τύπου τεκμηριωμένη σύμβαση .

12. Διαχείριση υπηρεσιών: Το σύνολο των δυνατοτήτων και των διαδικασιών που κατευθύνουν και να ελέγχουν τις δραστηριότητες και τους πόρους του φορέα παροχής υπηρεσιών για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών για την κάλυψη των απαιτήσεων των υπηρεσιών

13. Σύστημα διαχείρισης υπηρεσιών: Σύστημα διαχείρισης για να κατευθύνει και να ελέγχει τις δραστηριότητες παροχής υπηρεσιών διαχείρισης του παρόχου υπηρεσιών Ένα σύστημα διαχείρισης είναι ένα σύνολο αλληλένδετων ή αλληλεπιδρώντων στοιχείων για τη δημιουργία της πολιτικής και των στόχων και την επίτευξη των στόχων αυτών .Το SMS περιλαμβάνει όλες τις πολιτικές διαχείρισης των υπηρεσιών, τους στόχους, τα σχέδια, τις διαδικασίες, την τεκμηρίωση και τους πόρους που απαιτούνται για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών και την εκπλήρωση των απαιτήσεων σε αυτό το τμήμα του ISO / IEC 20000 .

14. Πάροχος υπηρεσιών: Οργάνωση ή μέρος μιας οργάνωσης που διαχειρίζεται και παρέχει μια υπηρεσία ή υπηρεσίες για τον πελάτη. Ένας πελάτης μπορεί να είναι εσωτερική ή εξωτερική οργάνωσης του φορέα παροχής υπηρεσιών .

15. Αίτηση υπηρεσίας: Αίτηση παροχής πληροφοριών, συμβουλών, την πρόσβαση σε μια υπηρεσία ή ένα προ-εγκεκριμένο αλλαγή

16. Απαίτηση υπηρεσίας: Ανάγκες του πελάτη και των χρηστών της υπηρεσίας, συμπεριλαμβανομένων των απαιτήσεων σε επίπεδο εξυπηρέτησης, και τις ανάγκες του παρόχου υπηρεσιών

17. Προμηθευτής: Οργάνωση ή μέρος μιας οργάνωσης που είναι εξωτερική οργάνωση του φορέα παροχής υπηρεσιών και να συνάπτει σύμβαση με τον πάροχο υπηρεσιών να συμβάλλουν στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών ή διαδικασιών.

18. Ανώτατα διοικητικά στελέχη: Πρόσωπο ή ομάδα ανθρώπων που διευθύνουν και ελέγχουν τον πάροχο υπηρεσιών στο υψηλότερο επίπεδο

19. Μετάβαση: Δραστηριότητες που εμπλέκονται στη μετακίνηση νέων ή τροποποιημένων δρομολογίων από και προς το ζωντανό περιβάλλον(Γιαννόπουλος 2001).

2.1 Εξασφάλιση των ηλεκτρονικών συναλλαγών

Οι κύριοι στόχοι της πολιτικής ασφάλειας του δικτύου θα πρέπει να είναι να διασφαλιστεί ότι η πρόσβαση στο δίκτυο της εταιρείας παρέχεται μόνο σε εξουσιοδοτημένους χρήστες, την ύπαρξη επαρκών ελέγχων για τη διαχείριση απομακρυσμένων χρηστών, ότι όλος ο εξοπλισμός μπορεί να αναγνωριστεί μοναδικά, ότι τα δίκτυα θα πρέπει να διαχωρίζονται με βάση τις ανάγκες και τα κατάλληλα πρωτόκολλα δρομολόγησης του δικτύου. Τυπικά πολιτικές δηλώσεις για την Ασφάλεια Δικτύων περιλαμβάνουν (Security updates: The upcoming revision of ISO/IEC 27001):

- Κατάλληλοι μηχανισμοί ελέγχου ταυτότητας πρέπει να χρησιμοποιηθούν για τον έλεγχο της πρόσβασης των απομακρυσμένων χρηστών .

- Κατανομή των δικαιωμάτων πρόσβασης στο δίκτυο πρέπει να παρέχεται σύμφωνα με τις απαιτήσεις των επιχειρήσεων και της ασφάλειας

- Έλεγχος ταυτότητας δύο παραγόντων πρέπει να χρησιμοποιείται για τον έλεγχο ταυτότητας των χρηστών που χρησιμοποιούν κινητά / απομακρυσμένα συστήματα

2.2 Μέτρα ασφαλείας

Η πολιτική ασφαλείας αφορά κάθε τεχνική και ενέργεια που περιορίζει τις ευπάθειες του πληροφοριακού συστήματος (Whitman & Mattord, 2013), (Peltier, 2013).

2.3 Tunneling

Το tunneling καλείται η διαδικασία χρήσης υποδομής των ηλεκτρονικών δικτύων για τη μετακίνηση στοιχείων μεταξύ των δικτύων. Τα στοιχεία προς μετακίνηση είναι δυνατόν να εφαρμόζονται σε πλαίσια ή πακέτα πρωτοκόλλου. τα οποία πραγματοποιούν διαδρομή ηλεκτρονικά σε ένα διαδικτυακό μονοπάτι το λεγόμενο tunnel. Από τη στιγμή που τα πακέτα φτάσουν στον προορισμό τους, τότε αφαιρούνται οι πρόσθετες κεφαλίδες. Ο όρος tunneling περικλείει όλη την παραπάνω διαδικασία (Whitman & Mattord, 2013).

Οι καινοτόμες τεχνολογίες tunneling είναι οι κάτωθι :

Point-to-Point Tunneling Protocol (PPTP).

IP Security (IPSec) Tunnel Mode.

Προκειμένου να εφαρμόζεται επιτυχές Tunneling είναι σκόπιμο και ο client και ο VPN server να εφαρμόζει όμοια πρωτόκολλα tunneling.

Για τις καινοτομίες του επιπέδου2 (Layer2) όπως η PPTP και L2TP η διαδικασία είναι η παρακάτω:

Και τα δύο άκρα του tunnel είναι σκόπιμο να έρθουν σε διαπραγμάτευση για τη ρύθμιση των παραμέτρων, όπως παραμέτρους κρυπτογράφησης και συμπίεσης. Στις περισσότερες περιπτώσεις τα στοιχεία που μετακινούνται μέσα από το tunnel κάνουν χρήση πρωτοκόλλων datagram-based.

2.4 IPsec

Η Ασφάλεια Πρωτοκόλλου Διαδικτύου (Internet Protocol Security - IPsec) είναι μία οικογένεια πρωτοκόλλων για την ασφαλή επικοινωνία του Πρωτοκόλλου Διαδικτύου (Internet Protocol – IP) μέσω του ελέγχου της ταυτότητας και της κρυπτογράφησης κάθε πακέτο IP μιας συνόδου επικοινωνίας. Η IPsec περιλαμβάνει πρωτόκολλα για την καθιέρωση αμοιβαίου ελέγχου ταυτότητας μεταξύ παραγόντων κατά την έναρξη της συνεδρίας και διαπραγμάτευσης των κρυπτογραφικών κλειδιών που θα χρησιμοποιηθούν κατά την διάρκεια της συνεδρίας. Η IPsec μπορεί να χρησιμοποιηθεί για την προστασία των ροών δεδομένων μεταξύ ενός ζεύγους κεντρικών υπολογιστών (*host-to-host*), μεταξύ ενός ζεύγους πυλών ασφαλείας (*network-to-network*), ή μεταξύ μιας πύλης ασφάλειας και ενός κεντρικού υπολογιστή (*network-to-host*). Η IPsec χρησιμοποιεί κρυπτογραφικές υπηρεσίες ασφαλείας για την προστασία των επικοινωνιών μέσω του IP. Η IPsec υποστηρίζει τον έλεγχο ταυτότητας σε επίπεδο δικτύου, τον έλεγχο ταυτότητας προέλευσης των δεδομένων, την ακεραιότητα των δεδομένων, την εμπιστευτικότητα των δεδομένων (κρυπτογράφηση), και την προστασία από την επανάληψη (Richardson, 2005).

Η IPsec είναι ένα σύστημα ασφάλειας από την πηγή δεδομένων στον προορισμό τους που λειτουργεί στο στρώμα του Διαδικτύου του Internet Protocol Suite, ενώ κάποια άλλα συστήματα ασφαλείας του Διαδικτύου που είναι σε ευρεία χρήση, όπως το Transport Layer Security (TLS) και το Secure Shell (SSH), λειτουργούν στα άνω στρώματα στο επίπεδο εφαρμογής. Ως εκ τούτου, μόνο η IPsec προστατεύει όλη την κυκλοφορία των αιτήσεων μέσω ενός δικτύου IP. Οι αιτήσεις μπορούν να ασφαλίζονται αυτόματα από την IPsec στο στρώμα IP(Peltier, 2013).

Τον Δεκέμβριο του 1993, το πρωτόκολλο κρυπτογράφησης λογισμικού (Software IP Encryption – swIPe) ερευνήθηκε στο Πανεπιστήμιο Κολούμπια και την AT&T Bell Labs από τον Ιωάννη Ιωαννίδη και άλλους.

Με την χρηματοδότηση από την κυβέρνηση Κλίντον στην φιλοξενία του ηλεκτρονικού ταχυδρομείου της whitehouse.gov (από την 1η Ιουνίου του 1993 έως 20 Ιανουαρίου του 1995) στην Trusted Information Systems, ο Wei Xu ξεκίνησε τον Ιούλιο του 1994, την έρευνα για την ασφάλεια IP, ενίσχυσε τα πρωτόκολλα IP και ανέπτυξε το IPSec στην πλατφόρμα BSDI, το οποίο και γρήγορα επεκτάθηκε για τα συστήματα Sun OS, HP UX και άλλα συστήματα UNIX. Μετά την επιτυχία του προϊόντος, ο Wei αντιμετώπιζε μια άλλη πρόκληση από την αργή απόδοση των υπολογιστών DES και Triple DES. Η κρυπτογράφηση του λογισμικού συναρμολόγησης δεν ήταν σε θέση να υποστηρίξει ακόμη και μια ταχύτητα T1 στην αρχιτεκτονική Intel 80386. Με την εξαγωγή των καρτών Crypto από την Γερμανία, ο Wei ανέπτυξε ένα αυτοματοποιημένο πρόγραμμα οδήγησης της συσκευής, γνωστό και ως plug-and-play σήμερα, στην ενσωμάτωση με το υλικό Crypto. Μετά την επίτευξη μίας απόδοσης πολύ υψηλότερη από ό,τι ένα T1s, ο Wei Xu έκανε τελικά το εμπορικό προϊόν πρακτικά εφικτό, το οποίο και κυκλοφόρησε ως μέρος του γνωστού τείχους προστασίας Gauntlet. Τον Δεκέμβριο του 1994, αναπτύχθηκε για πρώτη φορά στην παραγωγή για την διασφάλιση κάποιων απομακρυσμένων τοποθεσιών μεταξύ των ανατολικών και δυτικών παράκτιων πολιτειών των Ηνωμένων Πολιτειών (Whitman & Mattord, 2013).

Ένα άλλο Φορτίο ασφαλείας ενθυλάκωσης IP (Encapsulating Security Payload - ESP) ερευνήθηκε στο Εργαστήριο Ναυτικών Ερευνών, στο πλαίσιο μιας χορηγίας ερευνητικού έργου της DARPA, το οποίο δημοσιεύθηκε ανοιχτά από την Ομάδα Εργασίας SIPP IETF και συντάχθηκε το Δεκέμβριο του 1993 ως επέκταση ασφαλείας για το SIPP. Αυτό το ESP αρχικά προήλθε από το πρωτόκολλο SP3D του Υπουργείου Άμυνας των ΗΠΑ, αντί να προέλθει από το ISO Network-Layer Security Protocol (NLSP). Η προδιαγραφή του πρωτοκόλλου SP3D δόθηκε στην δημοσιότητα από το NIST, αλλά σχεδιάστηκε από το έργο Secure Data Network System του Υπουργείου Άμυνας των ΗΠΑ. Η επικεφαλίδα πιστοποίησης ταυτότητας (Security Authentication Header - AH) προήλθε εν μέρει από προηγούμενα IETF πρότυπα για τον έλεγχο ταυτότητας του απλού πρωτοκόλλου διαχείρισης δικτύου (Network Management Protocol - SNMP) έκδοση 2 (Κρυπτογραφία και Ασφάλεια Δικτύων) (Stallings, 2006).

Το 1995, η ομάδα εργασίας IPsec στο IETF άρχισε την δημιουργία μίας ανοιχτής και ελεύθερα διαθέσιμης και πιστοποιημένης έκδοσης πρωτοκόλλων που είχαν αναπτυχθεί στο πλαίσιο της σύμβασης με την NSA στο έργο Secure Data Network System (SDNS). Το έργο SDNS είχε ορίσει ένα πρωτόκολλο ασφαλείας Security Protocol Layer 3 (SP3) που είχε δημοσιευθεί από την NIST και αποτέλεσε επίσης την βάση του ISO Network Layer Security Protocol (NLSP). Η βασική διαχείριση του SP3 παρείχετο από το πρωτόκολλο

διαχείρισης κλειδιών (Key Management Protocol - KMP) το οποίο παρείχε μια βάση ιδεών στην επιτροπή IPsec για το επόμενο έργο (Richardson, 2005).

Η IPsec έχει τυποποιηθεί επίσημα από την Internet Engineering Task Force (IETF) σε μια σειρά από έγγραφα Request for Comments που αφορούν διάφορες συνιστώσες και προεκτάσεις και προσδιόρισε την ορθογραφία του ονόματος του πρωτοκόλλου να είναι *IPsec*.

Η IPsec είναι ένα ανοιχτό πρότυπο. Η IPsec χρησιμοποιεί τα ακόλουθα πρωτόκολλα για την εκτέλεση διαφόρων λειτουργιών:

• Επικεφαλίδες πιστοποίησης ταυτότητας (Authentication Headers - AH): παρέχουν χωρίς σύνδεση ακεραιότητα των δεδομένων και έλεγχο ταυτότητας προέλευσης δεδομένων για διαγράμματα δεδομένων IP (datagrams) και παρέχουν προστασία από επιθέσεις επανάληψης.

• Φορτία ασφαλείας ενθυλάκωσης (Encapsulating Security Payload - ESP) παρέχουν εμπιστευτικότητα, έλεγχο ταυτότητας προέλευσης των δεδομένων, ακεραιότητα των δεδομένων χωρίς σύνδεση, την υπηρεσία anti-replay (μια μορφή ακεραιότητας της μερικής ακολουθίας) και περιορισμένη εμπιστευτικότητα στην ροή της κυκλοφορίας δεδομένων.

• Συσχετισμοί ασφαλείας (Security Associations - SA) παρέχουν την δέσμη των αλγορίθμων και των δεδομένων που παρέχουν τις παραμέτρους που είναι αναγκαίες για την λειτουργία των AH ή/και του ESP. Ο συσχετισμός ασφαλείας του Διαδικτύου και το πρωτόκολλο διαχείρισης κλειδιών (ISAKMP) παρέχουν ένα πλαίσιο για τον έλεγχο ταυτότητας και την ανταλλαγή κλειδιών, με πραγματικά επικυρωμένο υλικό κλειδιών να παρέχεται είτε με χειροκίνητη ρύθμιση με προ-κοινόχρηστα κλειδιά, με Internet Key Exchange (IKE και IKEv2), Kerberized Internet Negotiation of Keys (KINK), ή εγγραφές IPSECKEY DNS.

Η επικεφαλίδα πιστοποίησης ταυτότητας (AH) είναι μέλος του πρωτοκόλλου IPsec. Η AH εγγυάται την χωρίς σύνδεση ακεραιότητα και τον έλεγχο ταυτότητας προέλευσης των δεδομένων των πακέτων IP. Περαιτέρω, μπορεί προαιρετικά να προστατεύσει από επιθέσεις επανάληψης χρησιμοποιώντας την τεχνική του κυλιόμενου παραθύρου (sliding window technique) και την απόρριψη των παλαιών πακέτων.

• Στο IPv4, η AH προστατεύει το φορτίο IP και όλα τα πεδία επικεφαλίδας ενός IP datagram εκτός από τα μεταβλητά πεδία (δηλαδή εκείνα που ενδέχεται να μεταβληθούν κατά την μεταφορά), καθώς επίσης και τις επιλογές IP, όπως η επιλογή IP Security (RFC 1108). Μεταβλητά (και ως εκ τούτου χωρίς έλεγχο ταυτότητας) πεδία της κεφαλίδας IPv4 είναι τα DSCP/ToS, ECN, Flags, Fragment Offset, TTL και Header Checksum.

• Στο IPv6, η AH προστατεύει το μεγαλύτερο μέρος της βάσης της επικεφαλίδας IPv6, την ίδια την AH, τις μη μεταβλητές επεκτάσεις των επικεφαλίδων μετά την AH, και το φορτίο IP. Η προστασία για την επικεφαλίδα IPv6 εξαιρεί τα μεταβλητά πεδία: DSCP, ECN, Flow Label και Hop Limit.

Η AH λειτουργεί απευθείας πάνω από την IP, με την χρήση του αριθμού πρωτοκόλλου IP 51 (Hoffman, 2005).

Το παρακάτω διάγραμμα πακέτου AH δείχνει πώς κατασκευάζεται ένα πακέτο AH και πώς ερμηνεύεται (Whitman & Mattord, 2013):

Το φορτίο ενθυλάκωσης ασφάλειας (ESP) είναι ένα μέλος των πρωτοκόλλων IPsec. Στην IPsec παρέχει αυθεντικότητα προέλευσης, ακεραιότητα και προστασία της εμπιστευτικότητας των πακέτων. Το ESP υποστηρίζει επίσης τις διαμορφώσεις κρυπτογράφησης και ελέγχου ταυτότητας μόνο, αλλά η χρήση της κρυπτογράφησης χωρίς έλεγχο ταυτότητας δεν συνιστάται επειδή είναι μη ασφαλής. Σε αντίθεση με της Επικεφαλίδα πιστοποίησης ταυτότητας (AH), το ESP στην λειτουργία της μεταφοράς δεν παρέχει ακεραιότητα και πιστοποίηση ταυτότητας για το σύνολο του πακέτου IP. Ωστόσο, σε κατάσταση λειτουργίας διόδου (tunnel mode), όπου το σύνολο του αρχικού πακέτου IP είναι ενθυλακωμένο με ένα νέο πακέτο επικεφαλίδας που έχει προστεθεί, η προστασία ESP παρέχεται σε ολόκληρο το εσωτερικό του πακέτου IP (συμπεριλαμβανομένης της εσωτερικής επικεφαλίδας), ενώ η εξωτερική επικεφαλίδα (συμπεριλαμβανομένων τυχόν εξωτερικών επιλογών IPv4 ή επεκτάσεις επικεφαλίδων IPv6) παραμένει απροστάτευτο. Το ESP λειτουργεί απευθείας πάνω από την IP, με τη χρήση του αριθμού πρωτοκόλλου IP 50.

2.4.1 Συσχετισμός ασφαλείας

Η αρχιτεκτονική ασφαλείας IP χρησιμοποιεί την έννοια του συσχετισμού ασφαλείας ως βάση για την δημιουργία λειτουργιών ασφαλείας στην IP. Ένας συσχετισμός ασφαλείας είναι απλά η δέσμη των αλγορίθμων και παραμέτρων (όπως τα κλειδιά) που χρησιμοποιείται για την κρυπτογράφηση και τον έλεγχο ταυτότητας μίας συγκεκριμένης ροή προς μία κατεύθυνση. Ως εκ τούτου, σε διπλής κατεύθυνσης κυκλοφορίας υπό κανονικές συνθήκες, οι ροές εξασφαλίζονται με ένα ζεύγος συσχετισμών ασφαλείας.

Οι συσχετισμοί ασφαλείας συστάθηκαν με την χρήση του Συσχετισμού Ασφαλείας Διαδικτύου και το Πρωτόκολλο Διαχείρισης Κλειδιών (ISAKMP). Το ISAKMP τίθεται σε εφαρμογή με χειροκίνητη ρύθμιση με προ-κοινόχρηστα μυστικά, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK) και την χρήση των εγγραφών IPSECKEY DNS. Το RFC 5386 ορίζει την ασφάλεια Better-Than-Nothing Security (BTNS) ως μη εξουσιοδοτημένη λειτουργία της IPsec χρησιμοποιώντας ένα εκτεταμένο πρωτόκολλο IKE.

Για να αποφασιστεί ποια προστασία πρέπει να παρασχεθεί σε ένα εξερχόμενο πακέτο, η IPsec χρησιμοποιεί τον Δείκτη Παραμέτρων Ασφαλείας (Security Parameter Index - SPI), έναν δείκτη στη βάση δεδομένων συσχετισμού ασφαλείας (SADB), μαζί με την διεύθυνση προορισμού σε μια επικεφαλίδα πακέτου, τα οποία από κοινού προσδιορίζουν με μοναδικό τρόπο έναν συσχετισμό ασφαλείας για το συγκεκριμένο πακέτο. Μια παρόμοια διαδικασία εκτελείται για ένα εισερχόμενο πακέτο, όπου η IPsec συγκεντρώνει τα κλειδιά αποκρυπτογράφησης και επαλήθευσης από την βάση δεδομένων του συσχετισμού ασφαλείας.

Για πολλαπλούς παραλήπτες, ένας συσχετισμός ασφαλείας παρέχεται για την ομάδα, και αναπαράγεται σε όλους τους πιστοποιημένους παραλήπτες της ομάδας. Μπορεί να υπάρχουν περισσότεροι από έναν συσχετισμό ασφαλείας για μια ομάδα, χρησιμοποιώντας διαφορετικές SPI, επιτρέποντας έτσι πολλαπλά επίπεδα και σύνολα ασφαλείας μέσα σε μια ομάδα. Πράγματι, κάθε αποστολέας μπορεί να έχει πολλούς συσχετισμούς ασφαλείας, επιτρέποντας τον έλεγχο ταυτότητας, δεδομένου ότι ένας λήπτης μπορεί μόνο να γνωρίζει ότι κάποιος που γνωρίζει τα κλειδιά απέστειλε τα δεδομένα. Σημειώστε ότι το σχετικό πρότυπο δεν περιγράφει πώς επιλέγεται και αναπαράγεται ο συσχετισμός σε όλη την ομάδα. Υποτίθεται ότι ένας υπεύθυνος έχει κάνει την επιλογή.

2.4.2 Υλοποιήσεις λογισμικού

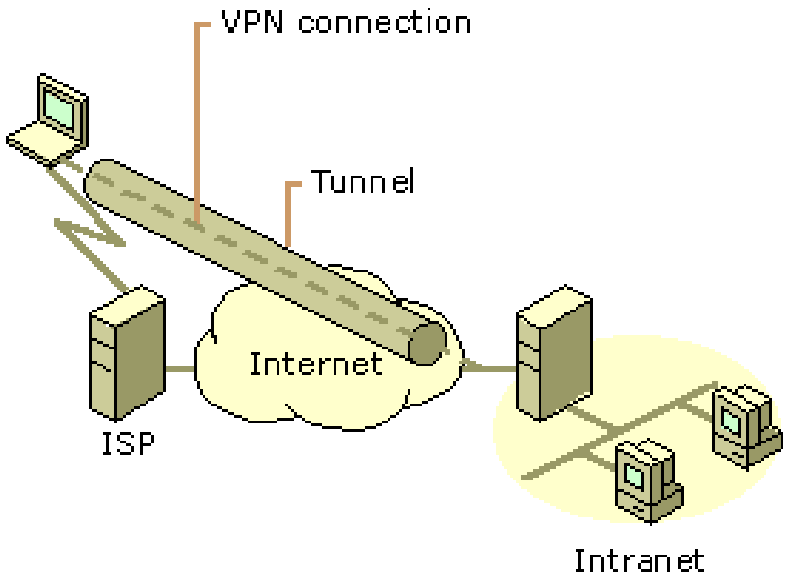
Η υποστήριξη IPsec συνήθως υλοποιείται στον πυρήνα με την διαχείριση κλειδιών και την διαπραγμάτευση ISAKMP/IKE να διεξάγεται από τον χώρο του χρήστη. Το «PF_KEY Key Management API, Version 2» χρησιμοποιείται συχνά προκειμένου η εφαρμογή διαχείρισης των κλειδιών στον χώρο εφαρμογή να επικαιροποιήσει τους συσχετισμοούς ασφαλείας της IPsec που είναι αποθηκευμένοι στον χώρο της υλοποίησης IPsec στον του πυρήνα. Οι υπάρχουσες υλοποιήσεις IPsec περιλαμβάνουν συνήθως ESP, AH και IKE έκδοση 2. Οι υπάρχουσες υλοποιήσεις IPsec για λειτουργικά συστήματα τύπου UNIX (π.χ. Solaris ή Linux), συνήθως περιλαμβάνουν την έκδοση 2 του PF_KEY (Whitman & Mattord, 2013).

Κεφάλαιο 3: Τύποι Δικτύων VPN

Ένα VPN δίνει τη δυνατότητα σε ένα ιδιωτικό intranet να επεκταθεί μέσω του Internet ή κάποιου άλλου δημόσιου δικτύου διατηρώντας την ιδιωτικότητά του και προσφέροντας υπηρεσίες όπως Business to Business (B2B) συνδέσεις με συνεργάτες και προμηθευτές για μια επιχείρηση ή σύνδεση των στελεχών με το εταιρικό δίκτυο (Nextep Broadband, 2001). Οι βασικοί τύποι VPN δικτύων ανάλογα με τον τρόπο χρήσης είναι οι εξής:

3.1 VPN για Απομακρυσμένη Πρόσβαση (Remote Access VPN)

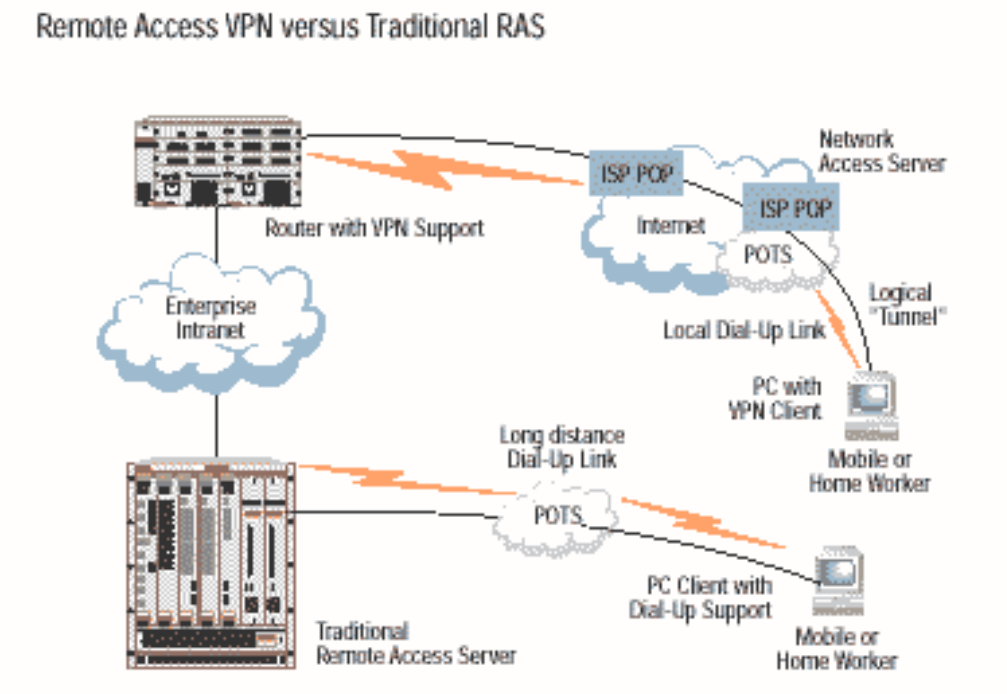
Η Απομακρυσμένη Πρόσβαση (Remote access) είναι η δυνατότητα σε ένα σύστημα Πελάτη – Εξυπηρετητή (Client Server) το σύστημα Πελάτης να μπορεί να συνδεθεί με τον Εξυπηρετητή από μια απομακρυσμένη τοποθεσία μέσω μιας ασφαλούς σύνδεσης. Τέτοιες VPN εφαρμογές δίνουν τη δυνατότητα σε χρήστες χρησιμοποιώντας μια dial up σύνδεση μέσω ενός ISP και του Internet να συνδέονται με το εταιρικό τους δίκτυο σαν να βρίσκονται στο χώρο της δουλειάς τους. Ο τύπος αυτός αναφέρεται και ως dial up VPN. Στο Σχήμα φαίνεται πως ένας χρήστης μπορεί να συνδεθεί με ένα εταιρικό εσωτερικό δίκτυο.



Σχήμα 3.1 Σύνδεση VPN απομακρυσμένου χρήστη με ένα intranet

Τα VPN τείνουν να αντικαταστήσουν τα παραδοσιακά συστήματα απομακρυσμένης Πρόσβασης αφού είναι όπως θα δούμε σαφώς πιο ευέλικτα και οικονομικά. Στις παλιές υλοποιήσεις χρησιμοποιούνταν ένας Εξυπηρετητής Πρόσβασης στο Δίκτυο (network access server - NAS) με τον οποίο ο χρήστης έπρεπε να επικοινωνήσει καλώντας τον από μακριά με ότι αυτό συνεπάγεται σαν κόστος κλήσης. Πλέον ο χρήστης καλεί

έναν τοπικό ISP και μέσω του Internet μπορεί να συνδεθεί με το απομακρυσμένο τοπικό Δίκτυο με τη χρήση ενός ειδικού software που υλοποιεί την εικονική ιδιωτική σύνδεση του χρήστη με τον VPN εξυπηρετητή του εταιρικού δικτύου.



Σχήμα 3.2 Υπηρεσία Remote Access

Η απομακρυσμένη σύνδεση χρησιμοποιείται κυρίως στις παρακάτω περιπτώσεις:

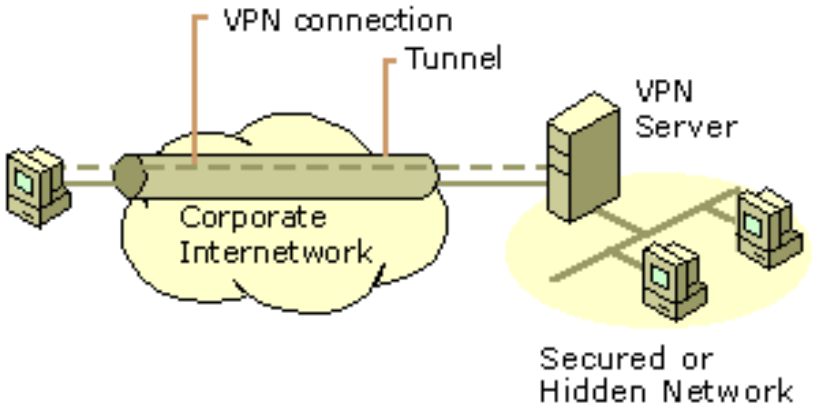
- Υπάλληλοι με τη χρήση φορητών Η/Υ με ενσωματωμένα modem συνδέονται με το εταιρικό δίκτυο.
- Χρήστες συνδέονται σε απομακρυσμένο δίκτυο χρησιμοποιώντας desktop PCs που είναι συνδεδεμένα με modem σε κάποιο δημόσιο δίκτυο όπως PSTN, ISDN ή ADSL.

Υπάρχουν δύο είδη απομακρυσμένων συνδέσεων, με τη χρήση είτε τοπικών συνδέσεων ή με απομακρυσμένες κλήσεις προς το εσωτερικό δίκτυο.

3.1.1 Intranet VPN – Σύνδεση μέσω ενός Intranet

Τα Intranet VPN αναφέρονται συχνά και σαν LAN to LAN VPN. Παρέχουν τη δυνατότητα σε κάποιο

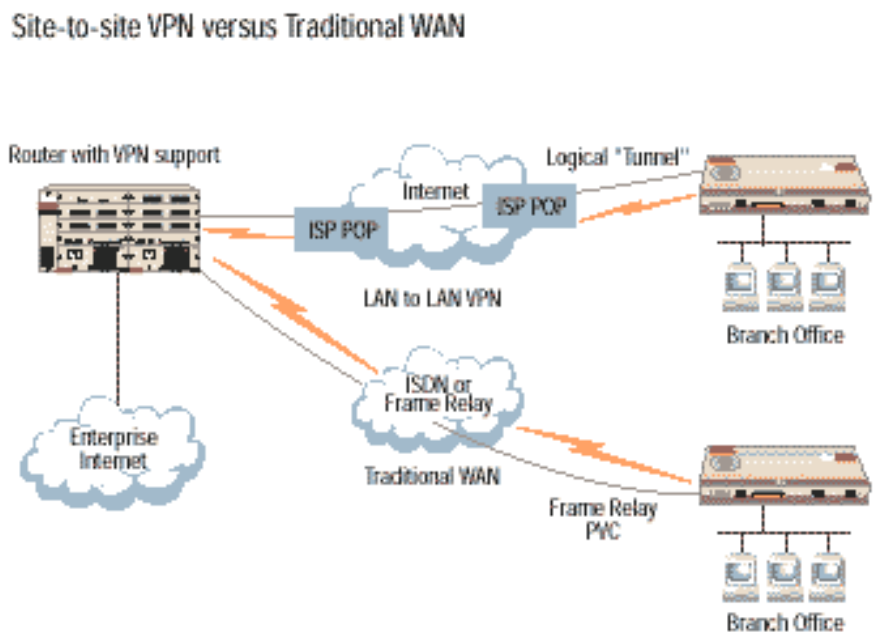
τοποθεσία ενός εταιρικού δικτύου να μπορεί να συνδεθεί με κάποιο άλλο τμήμα της εταιρίας με ασφαλή σύνδεση. Έτσι στην περίπτωση μιας τράπεζας το εταιρικό δίκτυο (Intranet) μπορεί να αποτελείται από πολλά τοπικά δίκτυα απομακρυσμένα το ένα από το άλλο τα οποία όμως είναι συνδεδεμένα με μια ασφαλή σύνδεση χρησιμοποιώντας ένα VPN. Το πρόβλημα διατήρησης ενός εταιρικού δικτύου το οποίο όμως τα διάφορα τμήματα είναι απομακρυσμένα μεταξύ τους είναι κοινό. Θα μπορούσε η σύνδεση των δικτύων να γίνει με κάποια παραδοσιακή μέθοδο Δικτύων Ευρείας περιοχής, γεγονός όμως που αυξάνει δραματικά το κόστος υλοποίησης ειδικά στην περίπτωση μικρών επιχειρήσεων. Επίσης η σύνδεση θα μπορούσε να γίνει με τη χρήση ενός απλού δρομολογητή ο οποίος συνδέει τα τοπικά δίκτυα χρησιμοποιώντας το Δημόσιο Δίκτυο όμως αυτό δε θα εξασφάλιζε σε καμιά περίπτωση την ιδιωτικότητα των δεδομένων. Συνεπώς η λύση βρίσκεται στη χρήση ενός VPN εξυπηρετητή ο οποίος μπορεί να συνδέει τα απομακρυσμένα τοπικά δίκτυα και να φροντίζει για την ασφάλεια των μεταδιδόμενων πληροφοριών καθώς και τη χρήση του δικτύου από εξουσιοδοτημένους απομακρυσμένους χρήστες.



Σχήμα 3.2.1 Σύνδεση VPN με ένα ασφαλές δίκτυο

Με τη χρήση ενός VPN ο διαχειριστής όχι μόνο ελέγχει την πρόσβαση στο δίκτυο μόνο από εξουσιοδοτημένους χρήστες αλλά μπορεί να αλλάξει δυναμικά τα δικαιώματα των απομακρυσμένων χρηστών ενώ παράλληλα αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται στις τεχνικές tunneling εγγυώνται το απόρρητο των πληροφοριών.

Σε μια υλοποίηση intranet VPN, οι ακριβές ιδιωτικές ή μισθωμένες γραμμές αντικαθίστανται είτε από μια σύνδεση μέσω Internet, ή μια ασφαλή σύνδεση που χρησιμοποιεί ένα δίκτυο Frame Relay ή ATM όπως φαίνεται στο Σχήμα.



Σχήμα 3.2.2 Intranet VPN

Με αυτό τον τρόπο ένα Intranet VPN μπορεί να προσφέρει σημαντική μείωση στο κόστος εγκατάστασης και συντήρησης σε σχέση με τα παραδοσιακά εταιρικά δίκτυα και να δώσει τη δυνατότητα υλοποίησης τέτοιων λύσεων σε μεγάλο αριθμό επιχειρήσεων από τις πιο μικρές (SOHO small office home office) μέχρι και τις πιο μεγάλες.

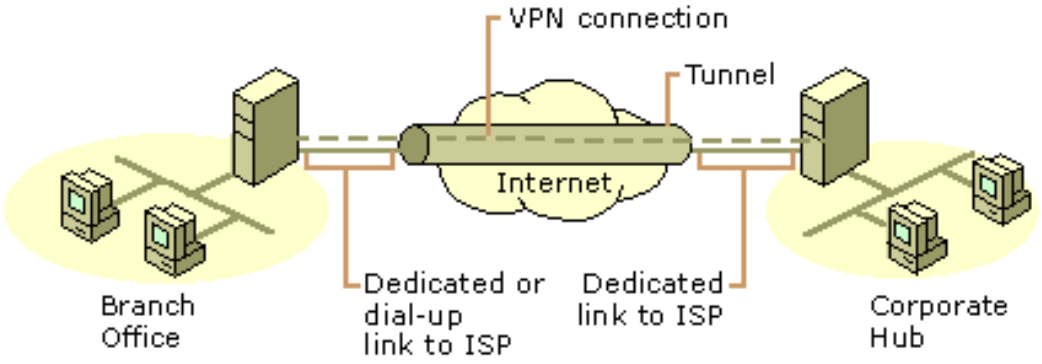
3.1.2 Extranet VPN

Ένα Extranet είναι ένα εταιρικό δίκτυο Intranet το οποίο δίνει τη δυνατότητα σε εξωτερικούς χρήστες να έχουν απομακρυσμένη πρόσβαση σε αυτό. Ένα Extranet VPN δίνει τη δυνατότητα σε μια επιχείρηση να προσφέρει ασφαλή απομακρυσμένη πρόσβαση σε πελάτες, προμηθευτές και συνεργάτες στο δίκτυό της. Στην περίπτωση των Extranet VPN, όπως θα δούμε εκτός από τις τεχνικές tunneling χρησιμοποιούνται και επιπλέον τεχνικές διασφάλισης της εμπιστευτικότητας των δεδομένων όπως είναι τα τείχη προστασίας (Firewalls).

3.1.3 Internet VPN

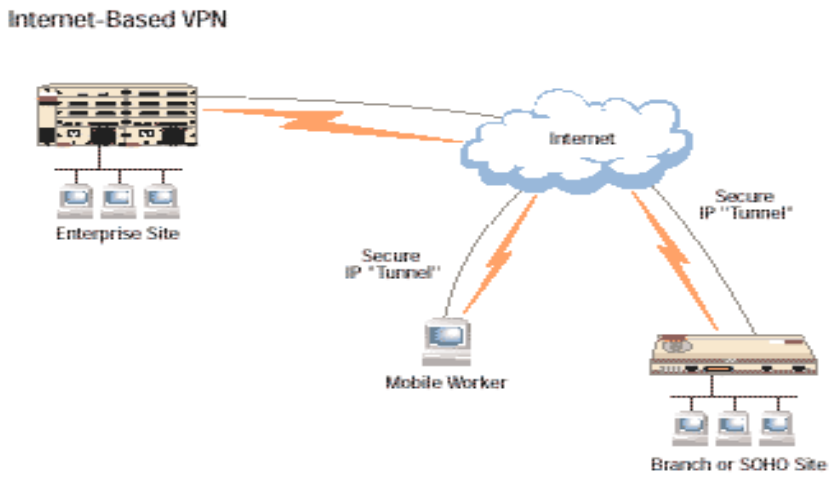
Σήμερα όταν αναφερόμαστε σε VPN, συνήθως εννοούμε Εικονικά Δίκτυα υλοποιημένα με βάση το Internet. Όπως θα δούμε υπάρχουν και άλλες υλοποιήσεις που χρησιμοποιούν μισθωμένες γραμμές T1 ή δίκτυα

Frame Relay. Όμως η υλοποίηση ενός δικτύου ευρείας περιοχής χρησιμοποιώντας τη λύση του Internet VPN μπορεί να μειώσει σημαντικά το κόστος του. Έτσι σε μια εταιρία με πολλά τμήματα, το κάθε τμήμα χρησιμοποιώντας κάποια πύλη μπορεί να συνδεθεί μέσω ενός τοπικού ISP με το Internet και μέσω αυτού να συνδεθεί με το τοπικό δίκτυο του άλλου τμήματος. Η σύνδεση της απομακρυσμένης τοποθεσίας με τον τοπικό της ISP μπορεί να γίνεται είτε με dial up σύνδεση ή να υπάρχει μια μόνιμη μισθωμένη γραμμή σύνδεσης. Το κεντρικό όμως εταιρικό δίκτυο το οποίο εξυπηρετεί τα απομακρυσμένα τμήματα θα πρέπει να χρησιμοποιεί μια μόνιμη σύνδεση σε 24ωρη βάση.



Σχήμα 3.2.3 Σύνδεση VPN ανάμεσα σε απομακρυσμένες τοποθεσίες

Η πρόσβαση στο Internet είναι πλέον εφικτή και στα πιο απομακρυσμένα σημεία του πλανήτη. Ανάλογα βέβαια με την υποδομή που διαθέτει κάθε γεωγραφικός τόπος μπορεί να επηρεαστεί άμεσα η απόδοση ενός Internet VPN, όμως η εξέλιξή του με ταχύ ρυθμό δίνει τη δυνατότητα σε μια εταιρία να το εκμεταλλευτεί για την υλοποίηση όχι μόνο του εξωτερικού αλλά και του εσωτερικού της δικτύου με μεγάλη ευελιξία και εξοικονόμηση χρημάτων.



Σχήμα 3.3 Internet VPN

3.4 Απαιτήσεις του VPN

Υπάρχουν κάποιες απαιτήσεις είτε τεχνολογικές ή πρακτικές οι οποίες πρέπει να ληφθούν σοβαρά υπόψη κατά την υλοποίηση ενός VPN. Για τη σωστή λειτουργία ενός τέτοιου δικτύου θα πρέπει να αντιμετωπισθούν κάποια προβλήματα που προκύπτουν κυρίως από το γεγονός ότι ιδιωτικά και εμπιστευτικά δεδομένα μεταδίδονται μέσω του δημόσιου δικτύου (Microsoft, 1999) Τα σημαντικότερα είναι τα εξής:

- Ασφάλεια (Security)

  Η ασφάλεια ίσως αποτελεί το σημαντικότερο θέμα που λαμβάνεται υπόψη κατά την υλοποίηση ενός Internet VPN. Χρησιμοποιούνται ποικίλες μέθοδοι για τη θωράκιση της ασφάλειας σε αυτά τα δίκτυα όπως η χρήση κρυπτογράφησης, ασφαλής ανταλλαγή κλειδιών, ταυτοποίηση ανά πακέτο ή ανά σύνοδο και πολλές άλλες. Αντίθετα με τις ιδιωτικές γραμμές επικοινωνίας, το δημόσιο δίκτυο μπορεί να δεχθεί πολύ πιο εύκολα επιθέσεις με σκοπό να διαβληθεί η ακεραιότητα ή η μυστικότητα ή διαθεσιμότητα των πληροφοριών (Data integrity, confidentiality and denial of services)

- Απόδοση και Ποιότητα Υπηρεσιών (Quality of Service QoS)

  Στις υπηρεσίες μετάδοσης Δεδομένων όπως στην περίπτωση των Frame Relay δικτύων, διασφαλίζονται με κάποιο τρόπο οι βασικές απαιτήσεις για διαθεσιμότητα των δεδομένων και έγκυρη και έγκαιρη μετάδοση τους. Οι προδιαγραφές αυτές ορίζονται από ένα Επίπεδο Συμφωνίας με τον παροχέα των υπηρεσιών (Service Level Agreement SLA). Παρά το γεγονός ότι τα VPN παρέχουν ένα ικανοποιητικό επίπεδο όσον αφορά την μετάδοση δεδομένων και την διαθεσιμότητά τους, σπάνια μπορούν να εγγυηθούν τη αποδοτικότητα του δικτύου και την αποφυγή καθυστερήσεων. Σχετική έννοια με αυτή της απόδοτικότητας ενός VPN δικτύου είναι και η ικανότητα εξοικονόμησης εύρους μετάδοσης (Bandwidth Reservation) με την οποία ένα σύστημα μπορεί να εξοικονομήσει μέρος του εύρους μετάδοσης για περιπτώσεις συμφόρησης του δικτύου και καθυστερήσεων.

- Επεκτασιμότητα (Scalability)

  Με τον όρο αυτό αναφερόμαστε στο κατά πόσο εύκολα ένα σύστημα μπορεί να επεκταθεί και να προσαρμοστεί στις αυξανόμενες ανάγκες. Ένα σύστημα που διαθέτει την ιδιότητα αυτή μπορεί εύκολα να καλύψει περισσότερες ανάγκες και να προσαρμοστεί με άλλα συστήματα. Η επεκτασιμότητα των VPN είναι πολύ μεγαλύτερη σε σχέση με τα παραδοσιακά ιδιωτικά δίκτυα στο παρελθόν.

- Διαχείριση

  Οι εφαρμογές VPN θα πρέπει να παρέχουν ένα αποδοτικό σύστημα διαχείρισης του δικτύου που θα επιτρέπει την εύκολη παραμετροποίηση και παρακολούθηση του συστήματος.

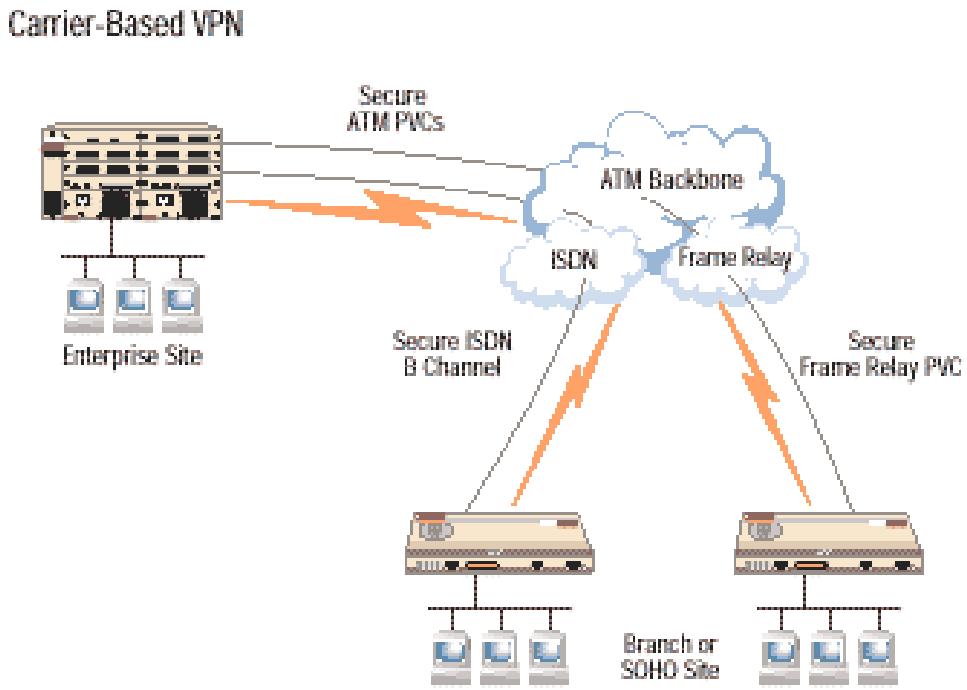
3.5 Τεχνολογίες VPN

Υπάρχουν όπως είπαμε διαφορές τεχνολογίες για την ανάπτυξη Εικονικών Ιδιωτικών Δικτύων (Virtual Private Network) τις οποίες και θα εξετάσουμε αναλυτικότερα. Οι παλαιότερες βασίζονται στη χρήση συνδέσεων ISDN, Frame Relay ή ATM ενώ οι πλέον σύγχρονες που θα εξετάσουμε και πιο λεπτομερώς βασίζονται στο Internet και στις τεχνικές IP tunneling για την ασφαλή μετάδοση των δεδομένων (Microsoft, 1999).

3.5.1 VPN βασισμένα σε ISDN, Frame Relay και ATM

Πριν την εξάπλωση του Internet, τα VPN βασίστηκαν σε συνδέσεις ISDN, Frame Relay και ATM και λειτουργούσαν με διαφορετικό τρόπο από ότι τα VPN με τη χρήση της τεχνικής IP tunneling. Το Εικονικό Ιδιωτικό δίκτυο αποτελούνταν από ένα ή περισσότερα μισθωμένα κυκλώματα τα οποία λειτουργούσαν όπως μια ξεχωριστή φυσική γραμμή επικοινωνίας. Ο παροχέας αυτής της σύνδεσης εγγυόταν την ασφάλεια της σύνδεσης εξασφαλίζοντας στο χρήστη αποκλειστική χρήση του κυκλώματος. Αυτά τα VPN ονομάζονται και εμπιστευτικά (trusted) VPN.

Δημόσια δίκτυα τύπου ISDN, Frame Relay ή ATM μπορούν να χρησιμοποιηθούν σαν έμπιστα VPN για να μεταδώσουν ποικίλα δεδομένα όπως πληροφορίες , φωνητικά δεδομένα ή δεδομένα ήχου και βίντεο παγκοσμίως. Έτσι μεγάλοι παροχείς υπηρεσιών δικτύου δημιούργησαν παγκόσμια δίκτυα βασισμένα σε Frame Relay τα οποία ήταν πολύ αποδοτικά. Για υπηρεσίες VPN χρησιμοποιήθηκαν κανάλια Β στην ISDN σύνδεση, καθώς και τα κυκλώματα Permanent Virtual Circuits (PVCs) ή Switched Virtual Circuits (SVCs) στις συνδέσεις ATM και Frame Relay για την αποκλειστική χρήση τους από τους χρήστες του VPN. Παρά το γεγονός ότι από μονή της η αποκλειστική χρήση ενός κυκλώματος για τη μετάδοση ιδιωτικών δεδομένων διασφαλίζει σε μεγάλο βαθμό την ασφάλεια των δεδομένων, αλγόριθμοι ταυτοποίηση χρηστών και κρυπτογράφησης χρησιμοποιήθηκαν επίσης στα έμπιστα VPN. Τα εικονικά δίκτυα που βασίζονται σε Frame Relay και ATM συνδέσεις ικανοποιούν διάφορα επίπεδα Ποιότητας Υπηρεσιών (QoS).



Σχήμα 3.4. Carrier Based VPN

Συγκεκριμένα η υλοποίηση ενός VPN με τη χρήση Frame Relay δικτύου θεωρείται σαν μια εύκολη και οικονομική τεχνολογία. Οι ιδιωτικές μισθωμένες γραμμές που απαιτούν μεγάλο κόστος εγκατάστασης και συντήρησης αντικαθίστανται από συνδέσεις δικτύων Frame Relay οι οποίες παρέχουν και μια ευελιξία στο εύρος ζώνης υποστηρίζοντας μεταβλητό ρυθμό μετάδοσης για την αποφυγή καθυστερήσεων σε κάποιο κύκλωμα. Υπάρχουν δύο τύποι υλοποίησης VPN μέσω Frame Relay:

- VPN με τη χρήση Frame Relay σύνδεσης χωρίς όμως τη χρήση της τεχνικής IP tunneling που θα εξετάσουμε παρακάτω. Όπως στις αποκλειστικές γραμμές σύνδεσης, έτσι και σε αυτή την υλοποίηση, η ασφάλεια και εμπιστευτικότητα των δεδομένων στηρίζεται στην αποκλειστική χρήση ενός κυκλώματος από τους εξουσιοδοτημένους χρήστες. Πρόκειται για συνδέσεις από Σημείο σε Σημείο (P2P) με τη χρήση ξεχωριστών εικονικών κυκλωμάτων.
- VPN σε Frame Relay σύνδεση με τη χρήση της τεχνικής IP tunneling. Οι συνδέσεις αυτές είναι επίσης από Σημείο προς Σημείο και χρησιμοποιούν ένα ξεχωριστό εικονικό κύκλωμα για τη σύνδεση. Επιπρόσθετα όμως χρησιμοποιείται και η τεχνική IP tunneling για να διασφαλιστεί ακόμα περισσότερα η ασφάλεια των μεταδιδόμενων πληροφοριών.

Τα κύρια πλεονεκτήματα από τη χρήση των VPN που βασίζονται στις συνδέσεις ISDN, Frame Relay και ATM είναι τα ακόλουθα:

- Οι συνδέσεις αυτές μπορούν να χρησιμοποιηθούν σε ένα μεγάλο φάσμα επικοινωνιών για τη μετάδοση ποικίλων πληροφοριών.
- Παρά το γεγονός ότι οι διεθνείς συνδέσεις Frame Relay είναι αρκετά ακριβές, είναι εύκολα διαθέσιμες.
- Θεωρούνται πολύ ασφαλή δίκτυα και τα θέματα ασφαλείας αντιμετωπίζονται από τον παροχέα των υπηρεσιών ή της σύνδεσης και όχι από το χρήστη.

Τα κύρια μειονεκτήματα είναι τα εξής:

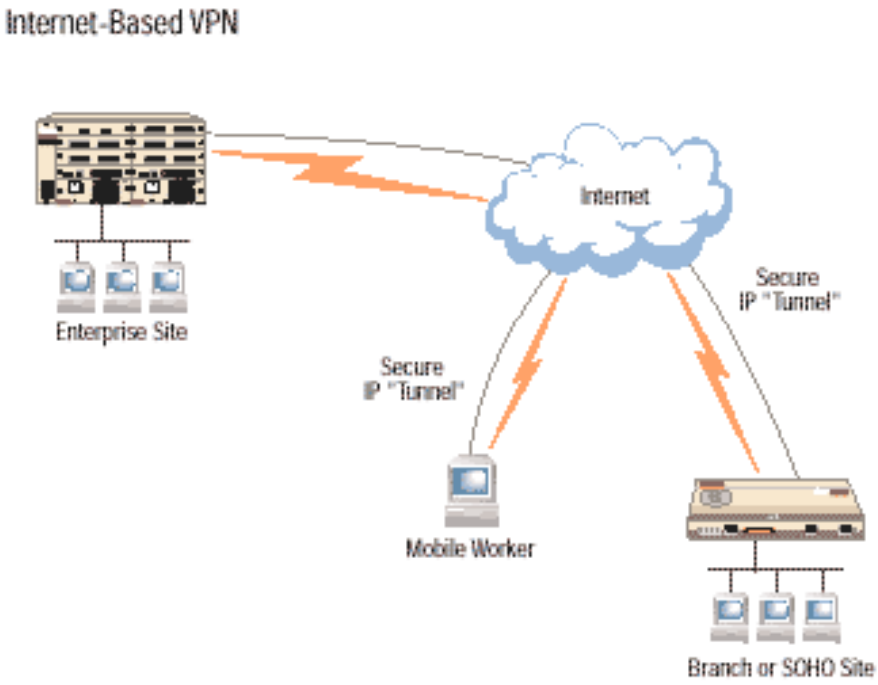
- Συγκριτικά με τα σύγχρονα IP VPN, τα παραδοσιακά VPN βασισμένα σε ISDN, Frame Relay ή ATM είναι πιο ακριβά ειδικά στην περίπτωση διεθνών συνδέσεων.
- Η διαθεσιμότητα των συνδέσεων αυτών δεν είναι τόσο ευρεία πλέον όπως οι συνδέσεις Internet από κάποιον ISP.
- Η υλοποίηση δικτύων extranet ειδικά σε περιπτώσεις ηλεκτρονικού εμπορίου με εξωτερικούς χρήστες όπως πελάτες και προμηθευτές είναι πολύ πιο δύσκολη σε σχέση με τη χρήση Internet VPN.

3.5.2 Εικονικά Ιδιωτικά Δίκτυα βασισμένα σε IP Tunnel

Τα VPN που βασίζονται στη μετάδοση με την τεχνική του IP tunnel λειτουργούν ως εξής: ενσωματώνουν ένα πακέτο δεδομένων σε ένα κοινό IP πακέτο το οποίο μεταδίδεται μέσω ενός IP δικτύου. Παρόλο που το πακέτο δεδομένων θα μπορούσε να μεταδοθεί με τη χρήση ενός οποιουδήποτε πρωτοκόλλου όπως το IPX, το AppleTalk, το SNA ή το DECnet, σήμερα συνήθως όταν ανφερόμαστε σε VPN, εννοούμε την υλοποίηση ενός Ιδιωτικού Δικτύου με τη χρήση του Internet σαν Δίκτυο Ευρείας Περιοχής (Wide Area Network WAN).

Συνεπώς η έννοια VPN σήμερα υποδηλώνει την υλοποίηση Ιδιωτικών Δικτύων όχι με τη χρήση απομακρυσμένων dial up συνδέσεων ή μισθωμένων γραμμών και Frame Relay συνδέσεων αλλά με τη χρήση τοπικών συνδέσεων προς κάποιον φορέα Παροχής Υπηρεσιών Internet (ISP) ή κάποιο άλλο σημείο παρουσίας υπηρεσιών Internet. Με αυτή την έννοια ένα VPN επιτρέπει σε ένα ιδιωτικό εσωτερικό δίκτυο (intranet) να μπορεί να επεκταθεί μέσω του Internet, υποστηρίζοντας ασφαλή μετάδοση δεδομένων όπως στην περίπτωση του ηλεκτρονικού εμπορίου.

Όσο το Internet μετατρέπεται όλο και περισσότερο σε ένα μέσο υλοποίησης ιδιωτικών δικτύων τόσο τα θέματα ασφαλείας όσον αφορά τη μετάδοση των ιδιωτικών δεδομένων γίνονται πιο επιτακτικά. Όπως θα εξετάσουμε στη συνέχεια, έχουν ήδη αναπτυχθεί πολλά πρωτόκολλα για την κωδικοποίηση των ιδιωτικών πληροφοριών έτσι ώστε αυτά να μπορούν να μεταδοθούν κρυπτογραφημένα μέσα από το δημόσιο δίκτυο και να αποκρυπτογραφηθούν στον παραλήπτη χωρίς να διαρρεύσουν σε μη εξουσιοδοτημένους χρήστες. Η τεχνική που χρησιμοποιείται λειτουργεί σαν ένα τούνελ μεταξύ του αποστολέα και του παραλήπτη, εμποδίζοντας κάθε εισβολέα από το να αποκτήσει την εμπιστευτική πληροφορία ή να την αλλοιώσει χωρίς αυτό να γίνει αντιληπτό. Στο παρακάτω Σχήμα παρουσιάζεται η δομή ενός Internet VPN το οποίο χρησιμοποιεί ασφαλή IP τούνελ για να συνδέσει χρήστες και συσκευές μέσω ενός Ιδιωτικού Δικτύου.



Σχήμα 3.5 Internet VPN

Τα Internet VPN που βασίζονται στην τεχνική του IP tunnel έχουν τα παρακάτω πλεονεκτήματα:

- Σημαντική μείωση του κόστους σύνδεσης και τηλεπικοινωνίας αφού οι απομακρυσμένες κλήσεις και οι μισθωμένες συνδέσεις αντικαθίσταται από τοπικές κλήσεις προς τους τοπικούς ISP.
- Πολύ ευέλικτη υλοποίηση απομακρυσμένης πρόσβασης από κινητούς υπολογιστές και απομακρυσμένες τοποθεσίες του ιδιωτικού δικτύου.
- Εύκολη υλοποίηση δικτύου extranet συνδέοντας μια επιχείρηση με τους πελάτες, τους προμηθευτές και τους εξωτερικούς συνεργάτες.

Τα κύρια βέβαια μειονεκτήματα των VPN με IP tunnel είναι τα εξής:

- Τα επίπεδα QoS είναι ακόμα χαμηλότερα σε σχέση με τις παραδοσιακές υλοποιήσεις κυρίως όσον αφορά τις καθυστερήσεις μετάδοσης δεδομένων.
- Κάθε VPN που βασίζεται σε ένα δημόσιο μέσο όπως το Internet απαιτεί πολύ υψηλότερα επίπεδα ασφαλείας κατά την ταυτοποίηση των χρηστών και την κωδικοποίηση των ιδιωτικών δεδομένων.

3.5.3 Διαδεδομένα Πρωτόκολλα VPN

Η βασική αρχή για την ανάπτυξη ενός VPN είναι η δημιουργία ενός τούνελ, μιας δηλαδή σύνδεσης μέσω του Δημοσίου Δικτύου όπως είναι το Internet όπου μπορεί αρχικά να γίνει μια ασφαλής ταυτοποίηση των μερών της σύνδεσης και στη συνέχεια μια ασφαλής μετάδοση των δεδομένων χωρίς να είναι δυνατή η προσβολή της ασφάλειας των μεταδιδόμενων δεδομένων. Τα πλέον πιο διαδεδομένα πρωτόκολλα ανάπτυξης VPN δικτύων είναι τα εξής:

- PPTP
- L2TP
- IPSec
- SSL

Τα πρώτα δύο όπως θα δούμε είναι ενσωματωμένα στην πλατφόρμα των Windows για την υλοποίηση VPN δικτύων ενώ τα άλλα δύο χρησιμοποιούνται από τα Windows για ταυτοποίηση και κρυπτογράφηση δεδομένων αλλά όχι σαν ξεχωριστές τεχνολογίες VPN. Παρόλα αυτά σε άλλες υλοποιήσεις τα πρωτόκολλα αυτά χρησιμοποιούνται από μόνα τους για την υλοποίηση Εικονικών Δικτύων και μάλιστα το IPSec φαίνεται να κερδίζει συνεχώς έδαφος έναντι των υπολοίπων στις ανεξάρτητες από Windows υλοποιήσεις.

- PPTP. Το πρωτόκολλο Point-to-Point Tunneling (PPTP), αναπτύχθηκε από τη Microsoft μαζί με άλλες εταιρίες και είναι η πιο διαδεδομένη τεχνολογία VPN στην πλατφόρμα των Windows αφού έχει συμπεριληφθεί από τις εκδόσεις Windows 9x και NT. Πρόκειται για μια επέκταση του διαδεδομένου πρωτοκόλλου Point-to-Point (PPP), που χρησιμοποιείται για τη μετάδοση πακέτων IP. Το PPTP χρησιμοποιεί τα ίδια πρωτόκολλα ταυτοποίησης με το PPP που θα εξετάσουμε στη συνέχεια όπως το PAP, CHAP, MS-CHAP και EAP. Το PPTP από μόνο του δεν υποστηρίζει κρυπτογράφηση γι αυτό και χρησιμοποιεί το πρωτόκολλο της Microsoft Point-to-Point Encryption (MPPE).Επειδή το client λογισμικό για την σύνδεση με τη χρήση του πρωτοκόλλου είναι ενσωματωμένο στα Windows, το μόνο

που απαιτείται είναι η εγκατάσταση του PPTP server. Παρόλα αυτά υπάρχουν client εφαρμογές για τα λειτουργικά Linux και Macintosh OS 9.

- L2TP.Το πρωτόκολλο Layer 2 Tunneling (L2TP) έχει αναπτυχθεί από τις εταιρίες Cisco και Microsoft συνδυάζοντας στοιχεία του PPTP με το παλαιότερο πρωτόκολλο Layer 2 Forwarding (L2F) της Cisco. Το πλεονέκτημα του είναι ότι μπορεί να χρησιμοποιηθεί και σε δίκτυα που δεν βασίζονται σε IP όπως τα ATM, frame relay και X.25. Όπως και το PPTP λειτουργεί όπως θα δούμε στο επίπεδο Σύνδεσης Δεδομένων του OSI και υποστηρίζεται από πολλά προϊόντα firewall όπως τα ISA Server, CheckPoint και Cisco.Το είναι ενσωματωμένο στα Windows 2000, XP και 2003 αλλά μπορεί να εγκατασταθεί η client εφαρμογή και στα παλαιότερα Windows (Windows 98, ME and NT 4.0). Το L2TP χρησιμοποιεί το IPSec και συγκεκριμένα το πρωτόκολλο Encapsulating Security Payload (ESP) για την κρυπτογράφηση των δεδομένων. Απαιτεί όπως θα δούμε τη χρήση ψηφιακών πιστοποιητικών για την ταυτοποίηση Παρέχει μεγαλύτερη ασφάλεια σε σύγκριση με το PPTP όσον αφορά την ακεραιότητα δεδομένων και την αποφυγή τροποποίησής τους κατά τη μετάδοση. Παρόλα αυτά λόγω του μεγαλύτερου επιπέδου ασφαλείας μπορεί να είναι ελαφρά πιο αργό σε θέμα απόδοσης από το PPTP.
- IPSec.Παρά το γεγονός ότι στα Windows το IPSec χρησιμοποιείται σαν πρωτόκολλο κρυπτογράφησης για το L2TP, μπορεί από μόνο του να χρησιμοποιηθεί ως πρωτόκολλο υλοποίησης δικτύου VPN ειδικά στην περίπτωση του site-to-site VPN όπου το IPSec λειτουργεί στο Επίπεδο 3 του μοντέλου OSI model. Εκτός της software υλοποίησης πολλές hardware υλοποιήσεις VPN εκμεταλλεύονται το IPSec όπως οι συγκεντρωτές VPN και τα PIX firewall της Cisco.Το IPSec δημιουργεί ένα tunnel για τη μετάδοση κρυπτογραφημένων πακέτων είτε ανάμεσα σε δύο gateway ή ανάμεσα σε έναν client υπολογιστή και ένα gateway. Λειτουργεί μόνο με IP δίκτυα και απαιτεί οι client υπολογιστές να έχουν τις κατάλληλες client software εφαρμογές. Η ταυτοποίηση των μερών υλοποιείται με το πρωτόκολλο Internet Key Exchange (IKE) που θα αναλύσουμε στη συνέχεια και που χρησιμοποιεί ψηφιακά πιστοποιητικά. Το IPSec υποστηρίζεται στα Windows 2000/XP/2003 και όχι στις παλαιότερες εκδόσεις των Windows.
- SSL. Το πρωτόκολλο Secure Sockets Layer (SSL) είναι ένα πρωτόκολλο ασφαλούς σύνδεσης που βρίσκει συνεχώς μεγαλύτερη εφαρμογή στην υλοποίηση VPN. Το μεγάλο του πλεονέκτημα είναι ότι δεν απαιτεί τη χρήση κάποιου ειδικού client λογισμικού αφού υποστηρίζεται από όλους Web browser. Αυτό βεβαία σημαίνει πως οι δυνατότητες εφαρμογών είναι πιο περιορισμένες από τα υπόλοιπα πρωτόκολλα. Επίσης αν οι εφαρμογές δεν είναι υλοποιημένες για την χρήση τους μέσω ενός browser τότε απαιτούν τη δημιουργία ενός interface έτσι ώστε να είναι προσβάσιμες από έναν browser. Τα SSL VPNs λειτουργούν σε ακόμα υψηλότερο επίπεδο από ότι το IPSec, στο Επίπεδο 4 δηλαδή στο Επίπεδο Συνόδου του μοντέλου OSI. Το SSL χρησιμοποιεί ψηφιακά πιστοποιητικά για την ταυτοποίηση των μερών της σύνδεσης.

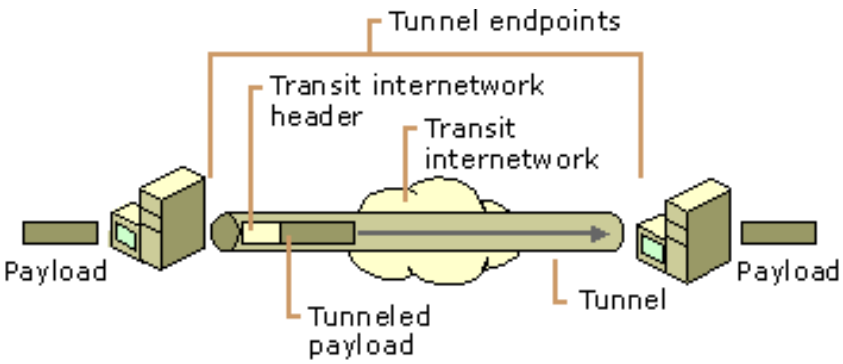
3.6 Tunneling

Γενικά με τον όρο tunneling εννοούμε τη μέθοδο κατά την οποία χρησιμοποιούμε την υποδομή ενός δικτύου για να μπορέσουμε μέσα από αυτό να μεταφέρουμε δεδομένα κάποιου άλλου δικτύου. Συγκεκριμένα είναι η εμφώλευση ενός πακέτου δεδομένων μέσα σε ένα άλλο πακέτο κατάλληλο για μεταφορά μέσω του Internet. Η διαδρομή μέσα από την οποία μεταδίδεται η εμφωλευμένη πληροφορία ονομάζεται Τούνελ. Έτσι η πληροφορία (payload) που πρόκειται να μεταδοθεί, όπως φαίνεται και στο Σχήμα δεν αποστέλλεται απευθείας στο Διαδίκτυο αλλά περιλαμβάνεται μέσα σε ένα πακέτο στο οποίο ενσωματώνεται και ένα header το οποίο περιέχει πληροφορίες για την δρομολόγηση του πακέτου και όλο αυτό ενθυλακώνεται μέσα στο IP πακέτο που πρόκειται να αποσταλεί μέσω του Internet. Τα ενθυλακωμένα πακέτα μεταδίδονται ουσιαστικά μέσα σε ένα τούνελ μέσα από το εξωτερικό δίκτυο (internetwork).

Για την υλοποίηση μιας σύνδεσης με τη μέθοδο tunneling, θα πρέπει και ο Πελάτης (tunnel client) και ο Εξυπηρετητής (tunnel server) να χρησιμοποιούν το ίδιο πρωτόκολλο tunneling. Από τη στιγμή που το tunnel έχει εγκατασταθεί, τα δεδομένα μπορούν να μεταδοθούν.

Σε γενικές γραμμές η διαδικασία είναι η εξής: Ο αποστολέας χρησιμοποιεί ένα πρωτόκολλο μεταφοράς δεδομένων για την αποστολή τους. Αρχικά δημιουργεί το tunneling πακέτο με τα δεδομένα και ενσωματώνει μια επικεφαλίδα (header) με πληροφορίες σχετικές με το πρωτόκολλο tunneling. Στη συνέχεια το πακέτο αυτό ενθυλακώνεται σε ένα εξωτερικό πακέτο κατάλληλο για το εξωτερικό δίκτυο. Τα δεδομένα με αυτή τη μορφή μεταδίδονται μέσω του εξωτερικού δικτύου και δρομολογούνται προς τον παραλήπτη. Κατά τη λήψη του πακέτου ακολουθείται η αντίστροφη διαδικασία. Τα πλαίσια του εσωτερικού πακέτου βγαίνουν από το πακέτο που μεταδόθηκε, η επικεφαλίδα αφαιρείται και τα δεδομένα δρομολογούνται στην τοποθεσία ή στο χρήστη στον οποίο απευθύνονται.

Στο Σχήμα περιγράφεται η διαδικασία εμφώλευσης μετάδοσης και εξαγωγής των πακέτων tunneling.



Σχήμα 3.6 Tunneling

Οι μέθοδοι Tunneling υπάρχουν από παλαιότερα. Μερικές από τις πρώτες τεχνολογίες που χρησιμοποιήθηκαν είναι οι εξής:

- IBM SNA tunneling μέσω IP δικτύων. Στο System Network Architecture (SNA) της IBM, τα δεδομένα στέλνονται μέσω ενός IP δικτύου και το πλαίσιο SNA ήταν ενθυλακωμένο μέσα σε μια επικεφαλίδα UDP ή IP.
- IPX tunneling σε δίκτυα Novell NetWare μέσω IP δικτύων. Όταν ένα πακέτο IPX στέλνεται μέσω ενός NetWare server ή ενός δρομολογητή IPX, τότε αυτός περικλείει το πακέτο μέσα σε μια UDP ή IP επικεφαλίδα και στη συνέχεια στέλενται μέσω του IP εξωτερικού δικτύου. Ο παραλήπτης αφαιρέι τη UDP ή IP επικεφαλίδα και αποστέλλει το πακέτο στον IPX προορισμό του.

Σήμερα χρησιμοποιούνται σύγχρονες τεχνικές tunneling. Οι πιο πρόσφατες χωρίζονται σε δύο μεγάλες κατηγορίες: Τα πρωτόκολλα tunneling Επιπέδου 2 και Επιπέδου 3 κατά αντιστοιχία προς το μοντέλο OSI (Open Systems Interconnection) (www.iec.org).

3.7 Πρωτόκολλα Tunneling

Όπως αναφέραμε υπάρχουν δύο ειδών πρωτόκολλα tunneling, τα Επιπέδου 2 και Επιπέδου 3. Τα πρωτόκολλα Επιπέδου 2 βασίζονται στο επίπεδο Σύνδεσης Δεδομένων και χρησιμοποιούν πλαίσια πρωτοκόλλου από Σημείο σε Σημείο (Point to Point Protocol PPP) σαν μονάδα μεταφοράς των δεδομένων. Τέτοια πρωτόκολλα είναι τα PPTP και L2TP (Cisco, 2004):

- PPTP (Point to Point Tunneling Protocol). Το PPTP επιτρέπει να μεταδίδονται μέσω δικτύων IP, IPX, ή NetBEUI κρυπτογραφημένα δεδομένα τα οποία ενσωματώνονται σε μια επικεφαλίδα IP για να σταλούν μέσω ενός IP διαδικτύου ή ενός δημόσιου IP διαδικτύου όπως το Internet.
- L2TP (Layer Two Tunneling Protocol). Το L2TP επιτρέπει να μεταδίδονται μέσω δικτύων IP, IPX, ή NetBEUI κρυπτογραφημένα δεδομένα επιτρέπει και να σταλούν μέσω οποιουδήποτε μέσου που υποστηρίζει μετάδοση Από Σημείο δε Σημείο όπως είναι τα δίκτυα IP, X.25, Frame Relay ή ATM.

Και στα δύο πρωτόκολλα το τούνελ (tunnel) είναι παρόμοιο με μια σύνοδο. Τα άκρα του τούνελ, συμφωνούν για την εγκατάστασης του τούνελ και τον ορισμό παραμέτρων όπως τη διευθυνσιοδότηση ή τις παραμέτρους κρυπτογράφησης και συμπίεσης. Συνήθως τα δεδομένα μεταδίδονται μέσα στο τούνελ με τη χρήση ενός πρωτοκόλλου που βασίζεται σε datagrams. Για τα πρωτόκολλα Επιπέδου 2 (Layer 2) χρησιμοποιείται ένα πρωτόκολλο συντήρησης με σκοπό τη δημιουργία συντήρηση και τερματισμό του τούνελ.

Τα πρωτόκολλα Επιπέδου 3 (Layer 3) βασίζονται στο επίπεδο Δικτύου κατά το OSI Μοντέλο και χρησιμοποιούν πακέτα. Πρωτόκολλα Επιπέδου 3 όπως το IPsec επιτρέπουν σε πακέτα IP να κρυπτογραφούνται και να ενθυλακώνονται σε μια επικεφαλίδα IP και στη συνέχεια να στέλνονται μέσω ενός εταιρικού IP διαδικτύου ή ενός δημόσιου IP διαδικτύου όπως το Internet. Οι τεχνολογίες tunneling Επιπέδου 3 γενικά προϋποθέτουν ότι όλες οι παράμετροι είναι προκαθορισμένες συνήθως με χειροκίνητο τρόπο και επιπλέον δεν περιλαμβάνουν κάποια διαδικασία συντήρησης του τούνελ.

3.8 Πρωτόκολλα Επιπέδου 2 (Layer 2 Tunneling Protocols)

Τα πρωτόκολλα PPTP και L2TP βασίζονται σε ένα καλά ορισμένο πρωτόκολλο μετάδοσης PPP Επιπέδου 2. Τα βασικά χαρακτηριστικά του πρωτοκόλλου είναι τα εξής:

- Ταυτοποίηση Χρήστη. Τα πρωτόκολλα tunneling Επιπέδου 3 υποθέτουν ότι τα δύο ακραία σημεία της μετάδοσης έχουν κάνει ταυτοποίηση χρήστη πριν δημιουργηθεί το τούνελ και συνεπώς οποιοσδήποτε χρήστης έχει πρόσβαση σε κάποιο από τα δύο σημεία μπορεί να στείλει δεδομένα μέσω του τούνελ. Γι αυτό και στην υλοποίηση του IPsec η αμοιβαία ταυτοποίηση των δύο μερών της μετάδοσης βασίζεται στη διαδικασία IKE (Internet Key Exchange). Από την άλλη τα πρωτόκολλα tunneling Επιπέδου 2 κληρονομούν τη μέθοδο ταυτοποίησης του PPP συμπεριλαμβανόμενης και της μεθόδου EAP (Extensible Authentication Protocol).
- Υποστήριξη καρτών Token. Η μέθοδος EAP προσφέρει στα πρωτόκολλα Επιπέδου 2 διάφορες τεχνικές ταυτοποίησης όπως κωδικούς μιας χρήσης, κρυπτογραφικούς υπολογισμούς και έξυπνες κάρτες.
- Δυναμική Διευθυνσιοδότηση. Η δυναμική απόδοση διεύθυνσης στο χρήστη βασίζεται στη μέθοδο NCP (Network Control Protocol).
- Συμπίεση Δεδομένων. Τα πρωτόκολλα Επιπέδου 2 υποστηρίζουν PPP μεθόδους συμπίεσης όπως τη MPPC (Microsoft Point to Point Compression) στην υλοποίηση tunelling με προϊόντα της Microsoft.
- Κρυπτογράφηση Δεδομένων. Τα πρωτόκολλα tunneling Επιπέδου 2 υποστηρίζουν κρυπτογράφηση που βασίζεται σε μεθόδους PPP. Η κρυπτογράφηση της Microsoft (Microsoft Point to Point Encryption MPPE) βασίζεται στον αλγόριθμο RSA/RC4 που θα εξετάσουμε παρακάτω.
- Διαχείριση Κλειδιών. Ο μηχανισμός κρυπτογράφησης στο Επίπεδο 2 βασίζεται στην παραγωγή ενός αρχικού κλειδιού κατά την ταυτοποίηση του χρήστη και την ανανέωσή του κατά περιόδους.
- Υποστήριξη πολλών πρωτοκόλλων μετάδοσης. Τα πρωτόκολλα Επιπέδου 2 υποστηρίζουν πολλαπλά πρωτόκολλα μετάδοσης δεδομένων όπως IP, IPX, NetBEUI κ.α. γεγονός που είναι σημαντικό για την ανάπτυξη ενός VPN σε κάποιο προϋπάρχουν εταιρικό δίκτυο.

Το πρωτόκολλο PPP σχεδιάστηκε για να στέλνει δεδομένα μέσω μόνιμων ή dial up συνδέσεων point to point. Η μέθοδος γενικά που χρησιμοποιεί είναι η εμφώλευση πακέτων IP, IPX ή NetBEUI μέσα σε πλαίσια PPP frames και η αποστολή των πλαισίων αυτών μέσω μιας σύνδεσης point to point. Το PPP χρησιμοποιείται μεταξύ ενός dial up Πελάτη και ενός Εξυπηρετητή NAS (Network Access Server). Τα βασικά βήματα για την εγκαθίδρυση μιας συνόδου PPP είναι τα ακόλουθα (Microsoft,1999):

1. Εγκαθίδρυση Σύνδεσης PPP.
2. Ταυτοποίηση Χρήστη.
3. Έλεγχος με Επιστρεφόμενη Κλήσης PPP.
4. Ενεργοποίηση Πρωτοκόλλου σε Επίπεδο Δικτύου.
5. Στάδιο Μεταφοράς Δεδομένων.

3.8.1 Εγκαθίδρυση Σύνδεσης PPP

Το πρωτόκολλο LCP (Link Control Protocol) χρησιμοποιείται για την εγκαθίδρυση, διατήρηση και τερματισμό μιας φυσικής σύνδεσης. Στη φάση Εγκαθίδρυσης της Σύνδεσης, εγκαθίσταται η σύνδεση και επιλέγονται τα πρωτόκολλα Ταυτοποίησης Χρηστές που θα χρησιμοποιηθούν στην αντίστοιχη φάση. Επιπλέον σε αυτό το στάδιο, λαμβάνεται η απόφαση για το αν τα δύο μέρη της σύνδεσης θα χρησιμοποιήσουν συμπίεση ή/και μεθόδους κρυπτογράφησης, οι οποίες θα επιλεχθούν στο στάδιο της Ενεργοποίησης του Πρωτοκόλλου Επιπέδου Δικτύου.

3.8.2 Ταυτοποίηση Χρήστη

Σε αυτή τη φάση, το σύστημα Πελάτης αποστέλλει στον Εξυπηρετητή Απομακρυσμένης Πρόσβασης τα διαπιστευτήριά του. Κατά την παραμετροποίηση της σύνδεσης PPP, ο Εξυπηρετητής του δικτύου (NAS) συλλέγει τα δεδομένα ταυτοποίησης και τα επικυρώνει στη βάση δεδομένων χρηστών. Η ταυτοποίηση χρηστών είναι κρίσιμης σημασίας για την εγγύηση της ακεραιότητας και εμπιστευτικότητας των δεδομένων.

Υπάρχουν διάφορα είδη επιθέσεων που μπορεί να δεχθεί μια ασφαλής σύνδεση για την απόκτηση πρόσβασης από μη εξουσιοδοτημένους χρήστες. Για παράδειγμα κάποιος εισβολέας μπορεί να παρακολουθήσει τα πακέτα που ανταλλάσσονται κατά τη διάρκεια μιας πετυχημένης σύνδεσης έτσι ώστε να τα αναπαράγει και να ταυτοποιηθεί σαν εξουσιοδοτημένος χρήστης. Επίσης ένας εισβολέας μπορεί να υποκλέψει τις παραμέτρους μιας ασφαλούς σύνδεσης και στη συνέχεια να αποσυνδέσει τον πραγματικό εξουσιοδοτημένο χρήστη για να συνδεθεί ο ίδιος. Τα πρωτόκολλο PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) και η έκδοση MS CHAP της Microsoft είναι χαρακτηριστικά δείγματα μεθόδων ταυτοποίησης PPP:

- PAP (Password Authentication Protocol). Πρόκειται για ένα απλό και όχι τόσο ασφαλές πρωτόκολλο σύμφωνα με το οποίο ο server πρόσβασης στο δίκτυο (NAS) ζητά από το χρήστη ένα όνομα χρήστη και έναν κωδικό και το πρωτόκολλο τα επιστρέφει χωρίς όμως να είναι κρυπτογραφημένα. Είναι πιθανόν λοιπόν ένας μη εξουσιοδοτημένος χρήστης να υποκλέψει το όνομα και κωδικό χρήστη και να τα χρησιμοποιήσει για να αποκτήσει πρόσβαση στο δίκτυο.
    - CHAP (Challenge Handshake Authentication Protocol). Πρόκειται για έναν μηχανισμό που χρησιμοποιεί κρυπτογράφηση για την ταυτοποίηση χρηστών. Ο server αποστέλλει μια κλήση στον απομακρυσμένο χρήστη η οποία αποτελείται από έναν κωδικό Συνόδου session ID) και ένα αυθαίρετο string κλήσης. Ο Πελάτης χρησιμοποιεί το μονόδρομο hash αλγόριθμο MD5 για να επιστρέψει στον server το όνομα χρήστη και κρυπτογραφημένα τον κωδικό Συνόδου και τον κωδικό χρήστη. Η μέθοδος CHAP είναι πιο αξιόπιστη γιατί το password δεν αποστέλλεται μέσω του δικτύου σαν απλό κείμενο. Το password χρησιμοποιείται για να δημιουργηθεί ένα κρυπτογραφημένο hash κλειδί από τα στοιχεία της αρχικής κλήσης. Καθώς ο server γνωρίζει τον κωδικό χρήστη μπορεί να δημιουργήσει επίσης το κλειδί και να συγκρίνει το αποτέλεσμα με το κρυπτογραφημένο κλειδί που απέστειλε ο χρήστης.
    - MS CHAP (Microsoft Challenge Handshake Authentication Protocol). Το MS CHAP είναι η υλοποίηση της Microsoft ενός μηχανισμού ταυτοποίησης χρήστη που βασίζεται στο CHAP προσφέροντας όμως ένα επιπλέον επίπεδο ασφαλείας. Ο server έχει τη δυνατότητα να αποθηκεύει τα passwords χρηστών όχι με τη μορφή απλού κειμένου αλλά κρυπτογραφημένα και επιπλέον το πρωτόκολλο προσφέρει επιπρόσθετους κωδικούς λάθους όπως κωδικό λήξης password και επιπρόσθετα κρυπτογραφημένα μηνύματα στην επικοινωνία μεταξύ client και server. Επιπλέον στο MS CHAP, ο client και ο NAS δημιουργούν ανεξάρτητα ο ένας από τον άλλον ένα αρχικό κλειδί το οποίο χρησιμοποιείται σε ακόλουθη κρυπτογράφηση δεδομένων από τον αλγόριθμο MPPE.

- EAP (Extensible Authentication Protocol). Το EAP αποτελεί ένα στάνταρτ της IETF σαν επέκταση του PPP, το οποίο υποστηρίζεται από τα Windows 2000. Παρέχει έναν αυθαίρετο μηχανισμό ταυτοποίησης χρήστη σε μια σύνδεση PPP. Το EAP παρέχει ειδικά modules για δυναμική προσθήκη ταυτοποίησης και στα δύο μέρη της σύνδεσης. Προσφέρει μεγάλη ευελιξία στη διαδικασία ταυτοποίησης.

- EAP TLS (Transport Level Security). Πρόκειται επίσης για ένα στάνταρτ της IETF που προσφέρει ταυτοποίησης με τη χρήση πιστοποιητικών Δημόσιου Κλειδιού. Στο EAP TLS, ο χρήστης χρησιμοποιεί ένα πιστοποιητικό για την ταυτοπόιησή του στον απομακρυσμένο server παρέχοντας έτσι ισχυρή απόδειξη της ταυτότητάς του. Επίσης ο server παρουσιάζει στον πελάτη επίσης ένα πιστοποιητικό έτσι ώστε ο πελάτης να διαβεβαιωθεί ότι είναι συνδεδεμένος με τον σωστό server. Τόσο το σύστημα πελάτης όσο και ο server χρησιμοποιούν κάποιο αναγνωρισμένο φορέα παροχής πιστοποιητικών. Το EAP TLS είναι το πρωτόκολλο που επίσης χρησιμοποιείται στα Microsoft Windows 2000. Όπως και στην περίπτωση του MS CHAP το πρωτόκολλο δημιουργεί κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται ακολούθως από τον αλγόριθμο MPPE.

3.8.3 Έλεγχος με Επιστρεφόμενη Κλήσης PPP

Στην υλοποίηση της Microsoft του πρωτοκόλλου PPP υπάρχει ένα επιπλέον προαιρετικό βήμα στη διαδικασία ταυτοποίησης. Σύμφωνα με το πρωτόκολλο CBCP (Callback Control Protocol) μετά τη φάση της ταυτοποίησης τα συστήματα Πελάτη και Εξυπηρετητή αποσυνδέονται. Στη συνέχεια ο Εξυπηρετητής NAS καλεί το σύστημα Πελάτη σε κάποια συγκεκριμένη τηλεφωνική σύνδεση και επαναλαμβάνει ένα επιπλέον στάδιο ταυτοποίησης.

3.8.4 Ενεργοποίηση Πρωτοκόλλου Επιπέδου Δικτύου

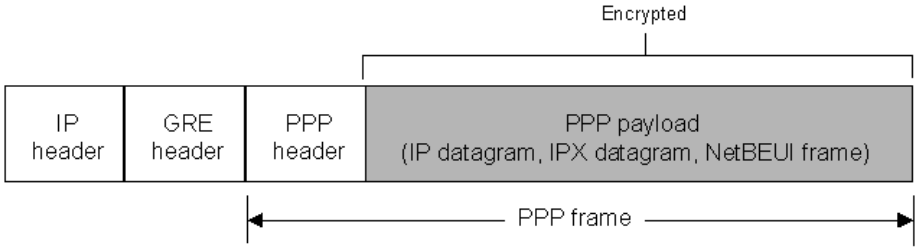
Όπως αναφέρθηκε, στο πρώτο στάδιο επιλέγονται και τα πρωτόκολλα ελέγχου του Δικτύου (Network control protocols NCPs) τα οποία μετά την ολοκλήρωση των προηγούμενων φάσεων ενεργοποιούνται, όπως για παράδειγμα το πρωτόκολλο διαχείρισης των διευθύνσεων IP (IP control protocol IPCP), το οποίο αποδίδει δυναμικά IP διεύθυνση στον απομακρυσμένο χρήστη.

3.8.5 Στάδιο Μετάδοσης Δεδομένων

Μόλις ολοκληρωθεί η διαπραγμάτευση μεταξύ client και server, το πρωτόκολλο PPP ξεκινά να μεταδίδει δεδομένα ανάμεσα στα δύο μέρη της σύνδεσης. Όπως ήδη αναφέραμε τα πακέτα δεδομένων εσωκλείονται σε μια επικεφαλίδα PPP, η οποία μεταφέρει τις πληροφορίες και αφαιρείται στον παραλήπτη. Αν έχει ήδη επιλεχθεί στο πρώτο στάδιο η χρήση κρυπτογράφησης ή συμπίεσης τότε τα δεδομένα μεταδίδονται συμπιεσμένα ή/και κρυπτογραφημένα.

3.9 PPTP Point to Point Tunneling Protocol

Το πρωτόκολλο PPTP (Point to Point Tunneling Protocol) είναι ένα πρωτόκολλο Επιπέδου 2 σύμφωνα με το οποίο πλαίσια PPP ενθυλακώνονται μέσα σε IP datagrams για να μεταδοθούν σε μέσω ενός δικτύου IP όπως είναι το Internet. Το PPTP μπορεί να χρησιμοποιηθεί είτε για VPN απομακρυσμένης πρόσβασης ή για VPN σύνδεση δρομολογητή με δρομολογητή. Το PPTP χρησιμοποιεί το πρωτόκολλο TCP σαν πρωτόκολλο συντήρησης του τούνελ και μια παραλλαγή του πρωτοκόλλου GRE (Generic Routing Encapsulation) για να ενθυλακώσει τα πλαίσια PPP. Τα δεδομένα των ενθυλακωμένων πλαισίων PPP μπορούν κρυπτογραφηθούν ή να συμπιεστούν. Το Σχήμα δείχνει τη δομή ενός πακέτου PPTP που περιέχει δεδομένα.



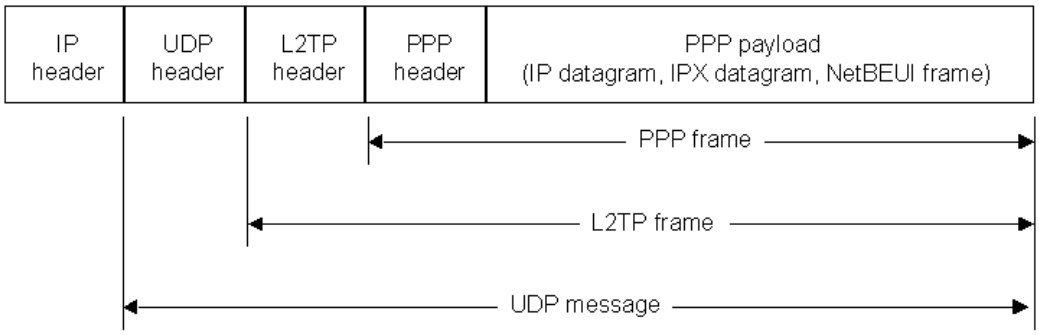
Σχήμα 3.7 Δομή του πακέτου PPTP

3.10 L2TP Layer Two Tunneling Protocol

Το πρωτόκολλο L2TP είναι ένας συνδυασμός των πρωτοκόλλων PPTP και L2F (Layer 2 Forwarding). Το πρωτόκολλο L2TP συνδυάζει τα καλύτερα στοιχεία των PPTP και L2F. Ενθυλακώνει πλαίσια PPP με σκοπό να μεταδίδονται μέσω δικτύων IP, X.25, Frame Relay ή ATM. Στην περίπτωση που χρησιμοποιείται το πρωτόκολλο IP για τη μετάδοση datagram , το L2TP μπορεί να χρησιμοποιηθεί σαν πρωτόκολλο tunneling μέσω του Internet.

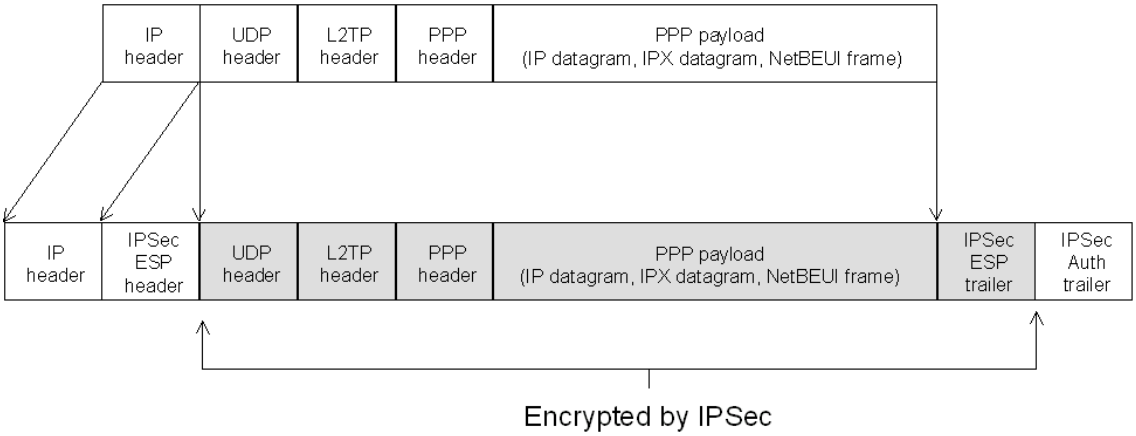
Το πρωτόκολλο L2TP μέσω δικτύων IP χρησιμοποιεί το πρωτόκολλο UDP και μια σειρά από L2TP μηνύματα για τη διατήρηση του τούνελ. Το L2TP χρησιμοποιεί επίσης το πρωτόκολλο UDP για να στέλνει τα ενθυλακωμένα πλαίσια PPP που περιέχουν τα δεδομένα. Οι μεταφερόμενες πληροφορίες των ενθυλακωμένων

πλαισίων PPP μπορούν να συμπιέζονται ή να κρυπτογραφούνται. Στο Σχήμα φαίνεται η δομή του πακέτου L2TP που περιέχει τα δεδομένα.



Σχήμα 3.8 Δομή του πακέτου L2TP

Για την κρυπτογράφηση των πακέτων L2TP χρησιμοποιείται το πρωτόκολλο IPsec Encapsulating Security Payload (ESP) το οποίο είναι γνωστό και ως L2TP/IPSec. Το αποτέλεσμα της εφαρμογής του πρωτοκόλλου ESP παρουσιάζεται στο Σχήμα.



Σχήμα 3.9 Δομή του πακέτου L2TP με τη χρήση IPSec EAP

3.11 IPsec - Internet Protocol Security Tunnel

Το IPsec είναι ένα πρωτόκολλο Επιπέδου 3 που υποστηρίζει την ασφαλή μετάδοση δεδομένων μέσω ενός IP δικτύου. Το IP Security σχεδιάστηκε από την IETF σαν ένας μηχανισμός για την ασφαλή μετάδοση δεδομένων από άκρο σε άκρο μέσω μιας IP σύνδεσης. Πέρα από τα θέματα ασφαλείας τα οποία και περιγράφονται στη συνέχεια, το IPsec ορίζει τη μορφή του πακέτου IP μέσω του IP τούνελ, το οποίο και

ονομάζεται IPsec Tunnel Mode. Το IPsec Tunnel Mode χρησιμοποιεί μια μέθοδο διαπραγμάτευσης θεμάτων ασφαλείας για να ενθυλακώσει κρυπτογραφημένα IP πακέτα και να μεταδοθούν μέσω ενός ιδιωτικού ή δημόσιου IP δικτύου. Τα κρυπτογραφημένα δεδομένα ενθυλακώνονται επιπλέον σε μια IP επικεφαλίδα τύπου απλού κειμένου και αποστέλλεται μέσω του δικτύου στον Εξυπηρετητή του τούνελ (tunnel server). Όταν ο εξυπηρετητής του τούνελ παραλάβει το datagram, το επεξεργάζεται και αφαιρεί την IP επικεφαλίδα απλού κειμένου. Στη συνέχεια αποκρυπτογραφεί τα περιεχόμενά της για να προκύψει το αρχικό IP πακέτο. Στη συνέχεια το IP πακέτο δρομολογείται κανονικά προς τον προορισμό του στο τελικό δίκτυο.

3.11.1 Είδη Τούνελ

Ένα IPsec τούνελ αποτελείται από έναν Πελάτη και έναν Εξυπηρετητή (tunnel client tunnel server) οι οποίοι είναι κατάλληλοι για τη χρήση του πρωτοκόλλου IPsec Tunneling και του μηχανισμού κρυπτογράφησης. Υπάρχουν δύο είδη τούνελ: τα προαιρετικά και τα υποχρεωτικά. Ένα προαιρετικό τούνελ εγκαθίσταται ανάμεσα σε ένα σύστημα Πελάτη και ένα σύστημα Εξυπηρετητή, όταν το σύστημα Πελάτη βρίσκεται στο ένα άκρο της σύνδεσης και λειτουργεί σαν Πελάτης στο τούνελ. Στην περίπτωση dial up σύνδεσης, ο πελάτης πρέπει να εκκινήσει μια dial up σύνδεση με το δίκτυο, συνδεόμενος συνήθως με έναν ISP για να αποκτήσει πρόσβαση στο Internet πριν το τούνελ μέσω του Internet δημιουργηθεί. Στην περίπτωση ενός υπολογιστή συνδεδεμένου σε LAN, ο υπολογιστής Πελάτης είναι ήδη συνδεδεμένος με το εταιρικό δίκτυο το οποίο μπορεί να δρομολογήσει τα ενθυλακωμένα πακέτα στον tunnel server του LAN.

Από την άλλη πλευρά, στην περίπτωση του υποχρεωτικού τούνελ, ο υπολογιστής Πελάτης δεν αποτελεί το ένα άκρο της σύνδεσης. Μια άλλη συσκευή αποτελεί το άκρο της σύνδεσης, η οποία λειτουργεί σαν Εξυπηρετητής dial up πρόσβασης (dial up access server) ανάμεσα στον υπολογιστή Πελάτη και τον Εξυπηρετητή του τούνελ (tunnel server). Ο Εξυπηρετητής αυτός είναι γνωστός και ως FEP (Front End Processor) στο πρωτόκολλο PPTP, ή LAC (L2TP Access Concentrator) στο πρωτόκολλο L2TP ή IP Security Gateway στο πρωτόκολλο IPsec (Microsoft 1999).

3.11.2 IP Security (IPsec)

Το πρωτόκολλο IPsec καθορίζει δύο βασικές λειτουργίες για τη διασφάλιση της εμπιστευτικότητας: τη κρυπτογράφηση των δεδομένων και την ακεραιότητά τους. Υπάρχουν δύο είδη επικεφαλίδων στο πρωτόκολλο IPsec:

- Authentication Header (AH). Η επικεφαλίδα αυτή αφορά την ταυτοποίηση της προέλευσης του μηνύματος και την ακεραιότητά του χωρίς τη χρήση κρυπτογράφησης.
- Encapsulating Security Payload (ESP). Η επικεφαλίδα αυτή παρέχει ταυτοποίηση και ακεραιότητα δεδομένων με κρυπτογράφηση. Στο πρωτόκολλο IPsec μόνο ο αποστολέας και ο παραλήπτης γνωρίζουν το κλειδί ασφαλείας.

3.11.3 Σύνδεση Ασφάλειας (Security Association)

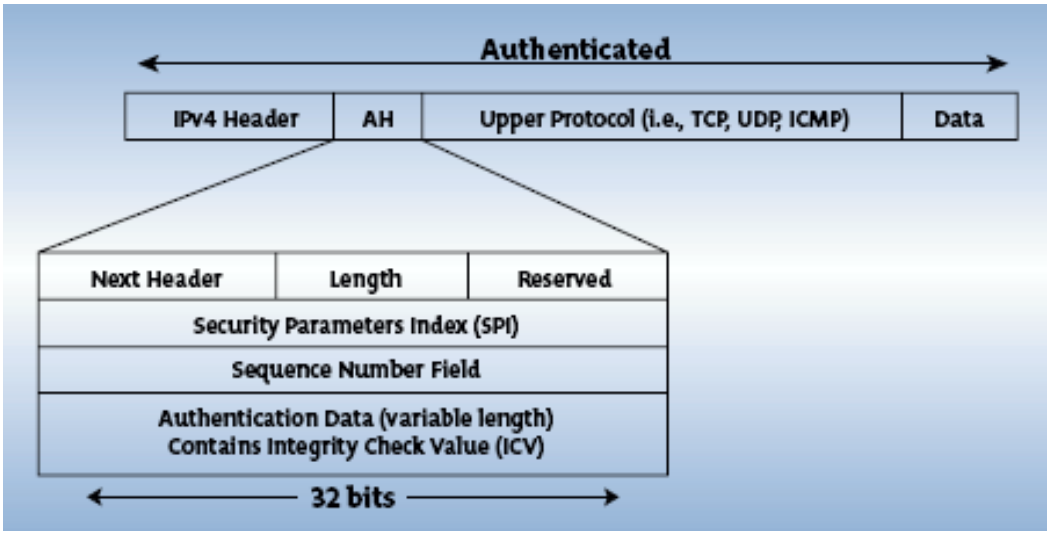
Το πρωτόκολλο IPsec ελέγχεται από μια πολιτική ασφαλείας σε κάθε υπολογιστή καθώς και μια παραμετροποιημένη σύνδεση ασφαλείας ανάμεσα στον αποστολέα και τον παραλήπτη. Η πολιτική ασφαλείας αποτελείται από ένα σύνολο φίλτρων και δικαιωμάτων ασφαλείας. Ο τρόπος με τον οποίο σχετίζονται οι οντότητες μεταξύ τους χρησιμοποιώντας το IPsec ορίζεται ως Σύνδεση Ασφάλειας (Security Association – SA). Πρόκειται για μια διαπραγμάτευση ανάμεσα στα δύο μέρη που χρησιμοποιούν το IPsec για το τρόπο με τον οποίο θα ασφαλίσουν την επικοινωνία μεταξύ τους. Τα επιμέρους θέματα που ορίζονται από τη Σύνδεση Ασφαλείας είναι τα εξής:

- IP Διεύθυνση Προέλευσης και Προορισμού
- Αλγόριθμος Ταυτοποίησης
- Αλγόριθμος Κρυπτογράφησης
- Τρόποι χρήσης και ανταλλαγής κλειδιών

Η Σύνδεση Ασφαλείας παρέχει τον τρόπο με τον οποίο τα δύο μέρη της σύνδεσης χρησιμοποιούν το πρωτόκολλο IPsec. Αφού οριστεί αυτή η Σύνδεση, τότε μπορεί να αρχίσει η μετάδοση δεδομένων εφαρμόζοντας την καθορισμένη ασφάλεια στα πακέτα. Η ασφάλεια μπορεί να διασφαλίσει μόνο την ακεραιότητα των μεταδιδόμενων πληροφοριών ή και να εφαρμόσει επιπλέον κρυπτογράφηση δεδομένων.

3.11.4 Επικεφαλίδα Ταυτοποίησης (Authentication Header)

Η ακεραιότητα και η ταυτοποίηση δεδομένων παρέχεται από μια επικεφαλίδα ταυτοποίησης τοποθετημένη ανάμεσα στην επικεφαλίδα IP και την επικεφαλίδα μεταφοράς του πακέτου. Η επικεφαλίδα ταυτοποίησης δεν κρυπτογραφεί το τμήμα δεδομένων του πακέτου. Τα μηνύματα που στέλνονται είναι απλού κειμένου και η Επικεφαλίδα Ταυτοποίησης διασφαλίζει την ταυτότητα προέλευσης των δεδομένων και την παράδοσή τους χωρίς αυτά να αλλοιωθούν κατά την μετάδοση. Η επικεφαλίδα περιέχει στοιχεία της ταυτοποίησης καθώς και έναν σειριακό αριθμό που δείχνει πόσα πακέτα έχουν μεταδοθεί, διασφαλίζει ότι το μήνυμα δεν έχει τροποποιηθεί και προφυλάσει από επίθεση αναπαραγωγής πακέτων για την απόκτηση πρόσβασης από μη εξουσιοδοτημένο χρήστη. Στο Σχήμα φαίνεται η δομή του μεταδιδόμενου πακέτου και της Επικεφαλίδας Ταυτοποίησης.

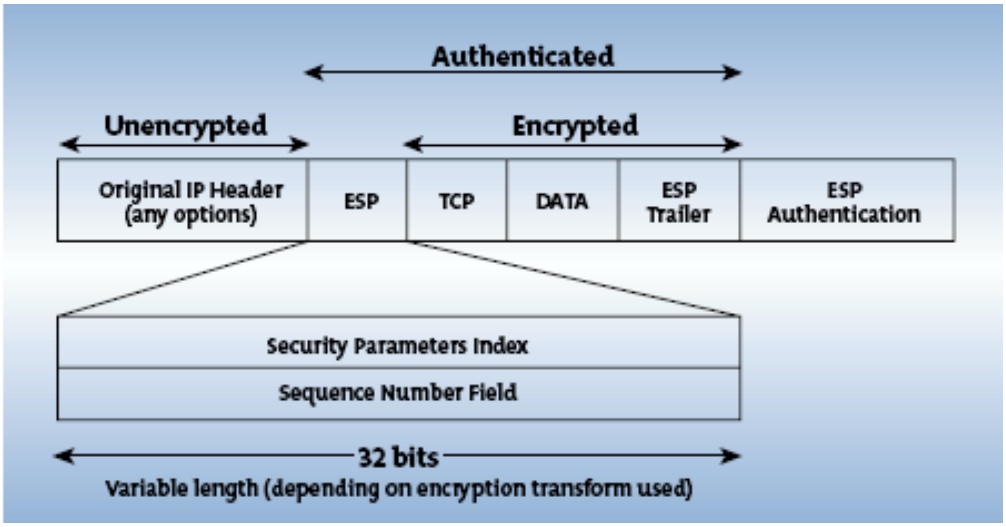


Σχήμα. Δομή Επικεφαλίδας Ταυτοποίησης

3.11.5 Ενθυλάκωση Δεδομένων Ασφαλείας (ESP)

Το πρωτόκολλο ESP (Encapsulating Security Payload) παρέχει έναν μηχανισμό κρυπτογράφησης των IP δεδομένων χρησιμοποιώντας έναν συμμετρικό αλγόριθμο κρυπτογράφησης. Επίσης το ESP παρέχει ταυτοποίηση και διασφάλιση ακεραιότητας δεδομένων όπως η επικεφαλίδα Ταυτοποίησης στην περίπτωση που απαιτείται εμπιστευτικότητα δεδομένων. Ο πιο κοινός αλγόριθμος κρυπτογράφησης που χρησιμοποιεί το ESP είναι ο DES (Data Encryption Standard). Όπως φαίνεται και στο Σχήμα η επικεφαλίδα ESP αποτελείται από ένα τμήμα Παραμέτρων Ασφαλείας και ένα σειριακό αριθμό και εισάγεται ανάμεσα στην επικεφαλίδα IP και το υπόλοιπο πακέτο. Το τμήμα Παραμέτρων Ασφαλείας (Security Parameters Index – SPI) και ο σειριακός

αριθμός έχουν τις ίδιες λειτουργίες όπως και στην περίπτωση της Επικεφαλίδας Ταυτοποίησης. Επιπλέον τα τμήματα TCP και δεδομένων είναι επίσης κρυπτογραφημένα.



Σχήμα. Δομή πρωτοκόλλου ESP

Στο IPsec τα IP πακέτα δεδομένων που αποστέλλονται μέσω του Internet πρώτα κρυπτογραφούνται και στη συνέχεια ενσωματώνονται σε ένα επιπλέον IP πακέτο. Τόσο οι δρομολογητές του Internet όσο και του εταιρικού δικτύου μπορούν να δουν μόνο τα εξωτερικά IP πακέτα, ενώ τα ενθυλακωμένα είναι προστατευμένα στο τμήμα δεδομένων του εσωτερικού IP πακέτου. Όπως ήδη αναφέραμε το πρωτόκολλο IPsec χρησιμοποιεί τον αλγόριθμο DES για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων.

3.11.6 Ανταλλαγή Κλειδιών

Η ανταλλαγή κλειδιών στο IPsec είναι ένα θέμα ζωτικής σημασίας. Τα κλειδιά μπορούν να δοθούν είτε δια χειρός ή με τη χρήση της μεθόδου IKE (Internet Key Exchange). Στην πρώτη περίπτωση τα κλειδιά εισάγονται με το χέρι στις συσκευές που θα χρησιμοποιήσουν το πρωτόκολλο IPsec χωρίς τη χρήση κρυπτογράφησης. Τα κλειδιά ορίζονται είτε από το διαχειριστή ή στέλνονται με e-mail. Ο τρόπος αυτός χρησιμοποιείται στις περιπτώσεις μικρών δικτύων, αλλά στις περιπτώσεις μεγαλύτερων δικτύων υπάρχει η ανάγκη για Σύνδεση Ασφαλείας κατά απαίτηση των συσκευών. Το πρωτόκολλο που χρησιμοποιείται είναι το IKE, το οποίο παλαιότερα αναφερόταν και σαν ISAKMP/Oakley. Το IKE είναι ένα πρωτόκολλο που βασίζεται στο UDP και χρησιμοποιεί τη θύρα 500 για την ανταλλαγή κλειδιών πελατών. Κατά τη διάρκεια μιας διαπραγμάτευσης IKE ένα ασφαλές τούνελ δημιουργείται ανάμεσα σε δύο μέρη. Οι υπολογιστές που πρόκειται να συνδεθούν συμφωνούν στις μεθόδους ταυτοποίησης και ασφάλειας δεδομένων, διεξάγουν την αμοιβαία

ταυτοποίηση ο ένας του άλλου και τέλος δημιουργούν ένα κοινό κλειδί για την κρυπτογράφηση των δεδομένων που θα ακολουθήσει. Το πρωτόκολλο IKE λειτουργεί σε τρεις διαφορετικές καταστάσεις:

- Κύρια Λειτουργία. Χρησιμοποιείται όταν δύο υπολογιστές επικοινωνούν για πρώτη φορά και διαπραγματεύονται τη Σύνδεση Ασφαλείας που θα χρησιμοποιήσουν.
- Επιθετική Λειτουργία. Πρόκειται για μια περιληπτική έκδοση της Κύριας Λειτουργίας.
- Γρήγορη Λειτουργία. Χρησιμοποιείται όταν η Σύνδεση Ασφαλείας έχει ή καθοριστεί με μια από τις προηγούμενες λειτουργίες και απαιτούνται επιπλέον ή πρόσθετες υπηρεσίες ασφαλούς σύνδεσης να καθοριστούν.

Η ταυτοποίηση IKE μπορεί να επιτευχθεί με διάφορες μεθόδους. Μια από τις μεθόδους είναι η διανομή εκ των προτέρων των κλειδιών όπου ο κάθε υπολογιστής φυλάσσει το ίδιο προκαθορισμένο μυστικό κλειδί. Με βάση το πρωτόκολλο IKE ένας υπολογιστής που συμμετέχει στη σύνδεση χρησιμοποιεί έναν hash κωδικό του κλειδιού για την ταυτοποίησή του. Ο άλλος υπολογιστής αποκρυπτογραφεί το hash κωδικό έτσι ώστε να συγκρίνει τα δύο κλειδιά. Στην περίπτωση του δημόσιου κλειδιού κάθε μέρος της σύνδεσης παράγει έναν τυχαίο αριθμό και ο κρυπτογραφεί με τη χρήση του Δημοσίου κλειδιού του άλλου μέρους της σύνδεσης και το αποστέλλει στο άλλο μέρος. Η ταυτοποίηση επιτυγχάνεται όταν το άλλο μέρος μπορεί να δημιουργήσει και να στείλει πίσω στο πρώτο μέρος έναν hash κωδικό του τυχαίου αριθμού που στάλθηκε αρχικά από το πρώτο μέρος.

Στην περίπτωση ψηφιακών υπογραφών, κάθε μέρος υπογράφει ψηφιακά ένα σύνολο δεδομένων και το αποστέλλει στο άλλο μέρος. Η μέθοδος είναι παρόμοια με τη μέθοδο του δημόσιου κλειδιού μόνο που σε αυτή την περίπτωση τόσο το δημόσιο κλειδί όσο και η ψηφιακή υπογραφή απαιτούν τη χρήση ψηφιακών πιστοποιητικών για την χαρτογράφηση των κλειδιών (Steffen, 2003).

3.12 Τείχος Προστασίας

Παρά το γεγονός ότι τα πρωτόκολλα tunelling Επιπέδου 2 και 3 προσφέρουν πολύ υψηλό επίπεδο ασφάλειας και πολλές υπηρεσίες κρυπτογράφησης και ταυτοποίησης, τα Τείχη Προστασίας χρησιμοποιούνται σε μεγάλο βαθμό στα Εικονικά Ιδιωτικά Δίκτυα. Ο όρος firewall έχει επικρατήσει τα τελευταία χρόνια σαν ένας από τους πιο καλούς τρόπους για να διατηρήσει κάποιος ασφαλή τα δεδομένα του στον υπολογιστή του, όταν αυτός είναι συνδεδεμένος στο διαδίκτυο. Το firewall, ή αλλιώς τείχος προστασίας, είναι μια συσκευή ή ένα λογισμικό το οποίο αναλαμβάνει να ελέγχει όλες τις πληροφορίες που φθάνουν στον υπολογιστή μας από τον "έξω" κόσμο καθώς επίσης και να ελέγχει ότι φεύγει από μέσα προς τα έξω χωρίς την άδειά μας. Υπάρχουν 3

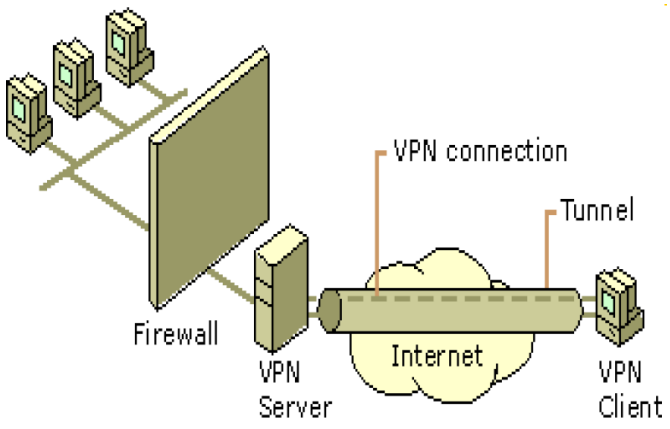
είδη τειχών προστασίας:

- Firewall φιλτραρίσματος πακέτων
- Proxy Firewall
- Stateful Inspection Firewall.

Στην περίπτωση του λογισμικού firewall, μπορούμε να καθορίσουμε τους υπολογιστές ή τις διευθύνσεις από τις οποίες μπορούμε να δεχόμαστε πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι. Η μεγάλη σημασία του firewall έγκειται στο ότι δεν μπορούμε να γνωρίζουμε απόλυτα τι λογισμικά υπάρχουν εγκατεστημένα στον υπολογιστή μας και ποιες "πόρτες" είναι ανοιχτές ειδικά στην περίπτωση που ο υπολογιστής είναι μολυσμένος από ένα worm το οποίο δίνει τη δυνατότητα σε κάποιον άλλο υπολογιστή να χρησιμοποιεί τους πόρους του.

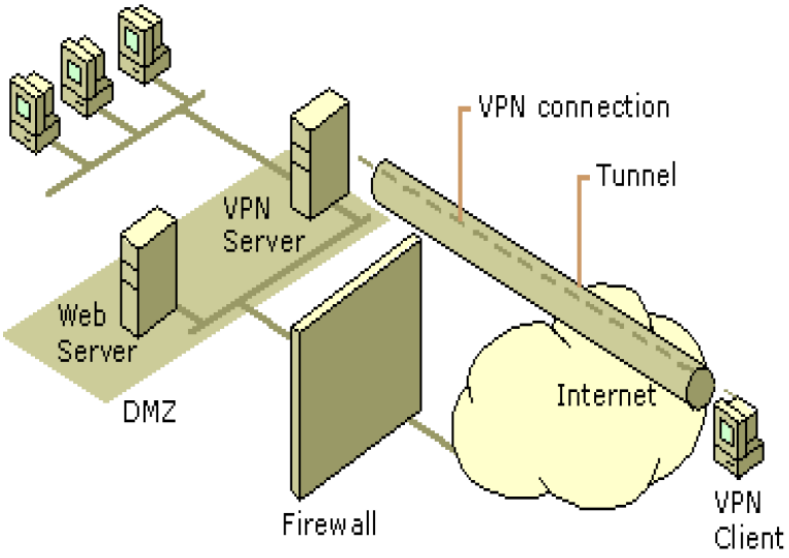
Το IPsec προσφέρει πολλές δυνατότητες ταυτοποίησης και κρυπτογράφησης. Παρόλα αυτά τα firewalls χρησιμοποιούνται αρκετά συχνά στις υλοποιήσεις VPN. Ανάλογα με την υλοποίηση υπάρχουν δύο προσεγγίσεις στη χρήση του firewall:

- Ο VPN server είναι εφαπτόμενος του Internet και το firewall είναι μεταξύ του VPN server και του Intranet.



Σχήμα 3.11 Firewall μεταξύ VPN server και Intranet

- Το firewall είναι εφαπτόμενο στο Internet και ο VPN server είναι μεταξύ του firewall και του Intranet.



Σχήμα 3.12 VPN server μεταξύ Firewall και Intranet

Τα πακέτα αποκρυπτογραφούνται και φιλτράρονται πριν να σταλούν στον παραλήπτη. Στην περίπτωση που υλοποιείται ένα extranet VPN τότε το firewall συνήθως τοποθετείται έξω από τον VPN server και προστατεύει από μη εξουσιοδοτημένες απόπειρες πρόσβασης. Πάντα βέβαια ενλογχεύει ο κίνδυνος κάποιος εισβολέας να ανακαλύψει κάποια τρύπα στο τείχος προστασίας και να επιτεθεί στο σύστημά μας (Nortel Networks, 2002).

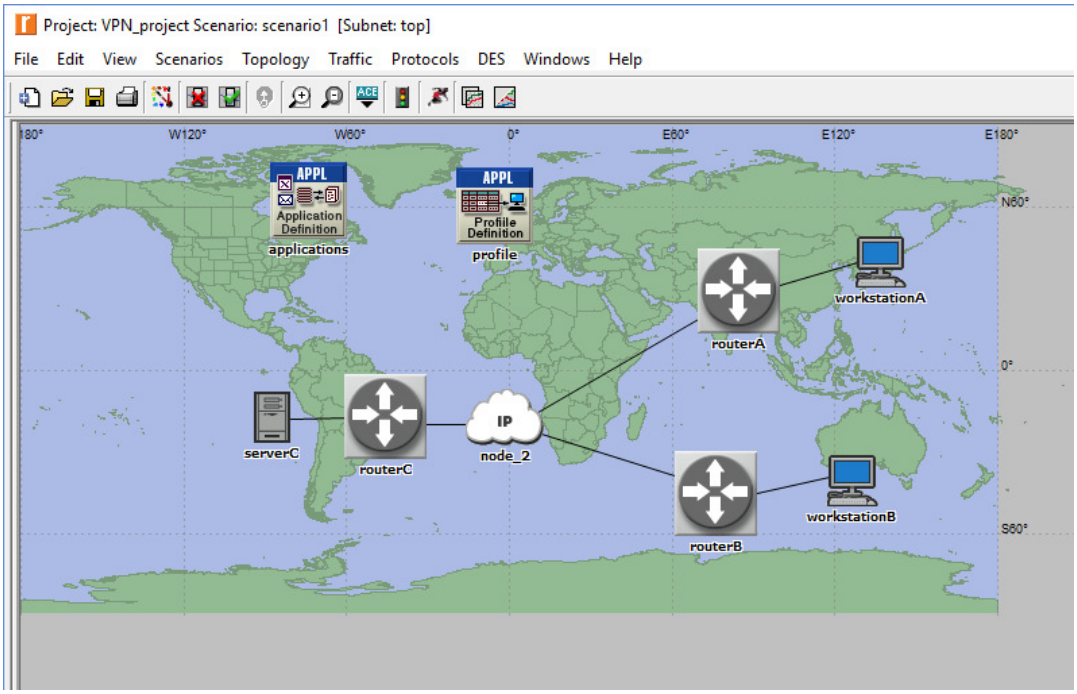
Κεφάλαιο 4: Σενάρια

Η σύνδεση μεταξύ των κόμβων του δικτύου έγινε με τη χρήση συνδέσεων **PPP_DS1.** Τα σενάρια που υλοποιήθηκαν είναι τρία, ένα σενάριο χωρίς κάποιο περιορισμό δικαιωμάτων στην πρόσβαση των σταθμών εργασίας και του server, ένα δεύτερο με τη χρήση τοίχου προστασίας (firewall) και τέλος με την χρήση ενός router που υλοποιεί πρωτόκολλο VPN.

4.1 Σενάριο 1

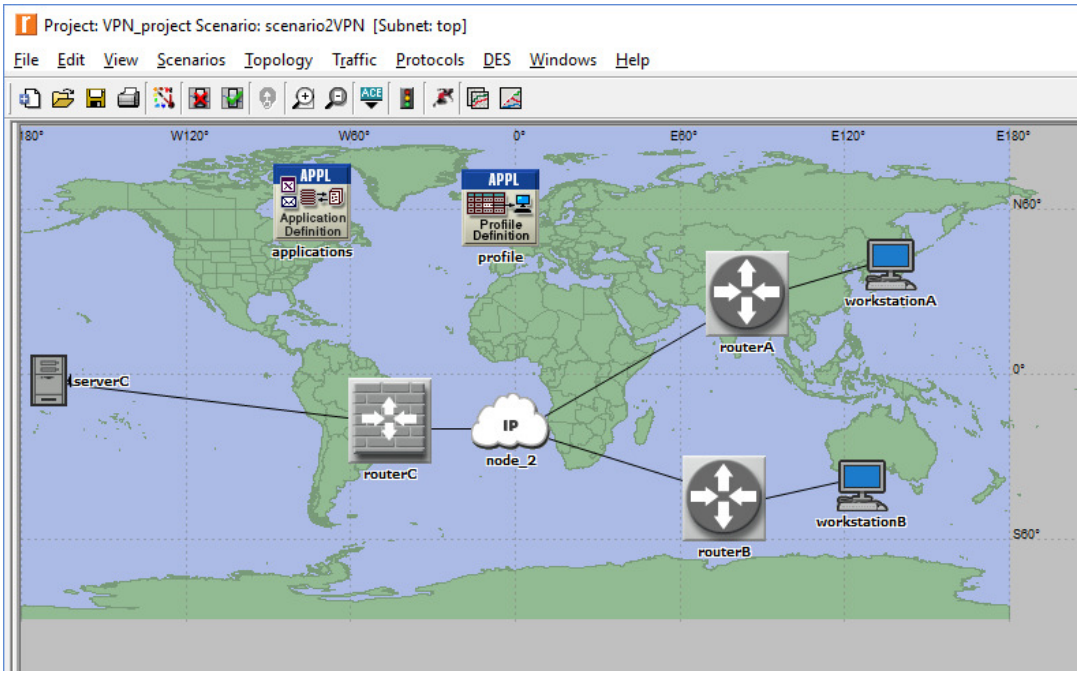
Στο σενάριο 1 η τοπολογία είναι η εξής:

Δύο σταθμοί εργασίας, οι workstationA και workstationB συνδέονται μέσω κάποιου router (routerA και routerB αντίστοιχα) στο internet. Επίσης υπάρχει ένας απομακρυσμένος server ο οποίος και αυτός είναι συνδεδεμένος στο διαδίκτυο μέσω του routerC.



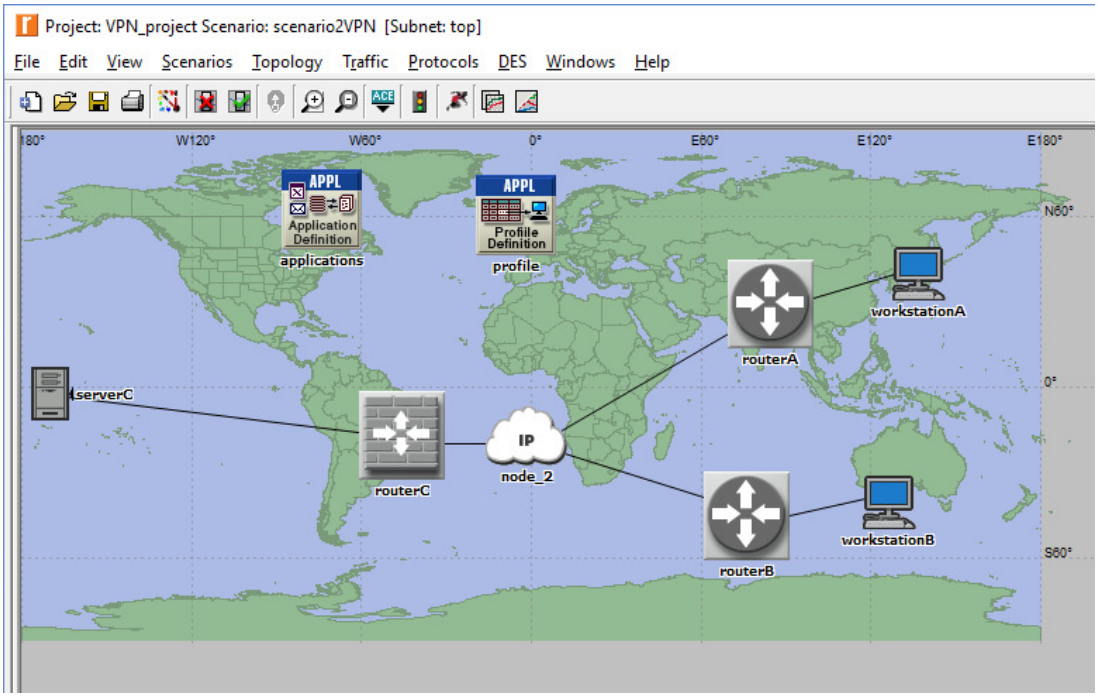
4.2 Σενάριο 2

Στο δεύτερο σενάριο οι δύο σταθμοί εργασίας, workstationA και workstationB συνδέονται μέσω κάποιου router (routerA και routerB αντίστοιχα) στο internet. Ο server είναι συνδεδεμένος στο router C το οποίο και λειτουργεί ως **firewall** για τον έλεγχο των εισερχομένων και εξερχομένων request.



4.3 Σενάριο 3

Στο τελευταίο σενάριο ανάμεσα στον server και στον router C παρεμβάλλεται ένα επιπλέον router για την υλοποίηση του πρωτοκόλλου VPN. Η υλοποίηση γίνεται με τη χρήση MPLS VPN.



Για τα στατιστικά στις δοκιμές επιλέχθηκαν τα εξής:

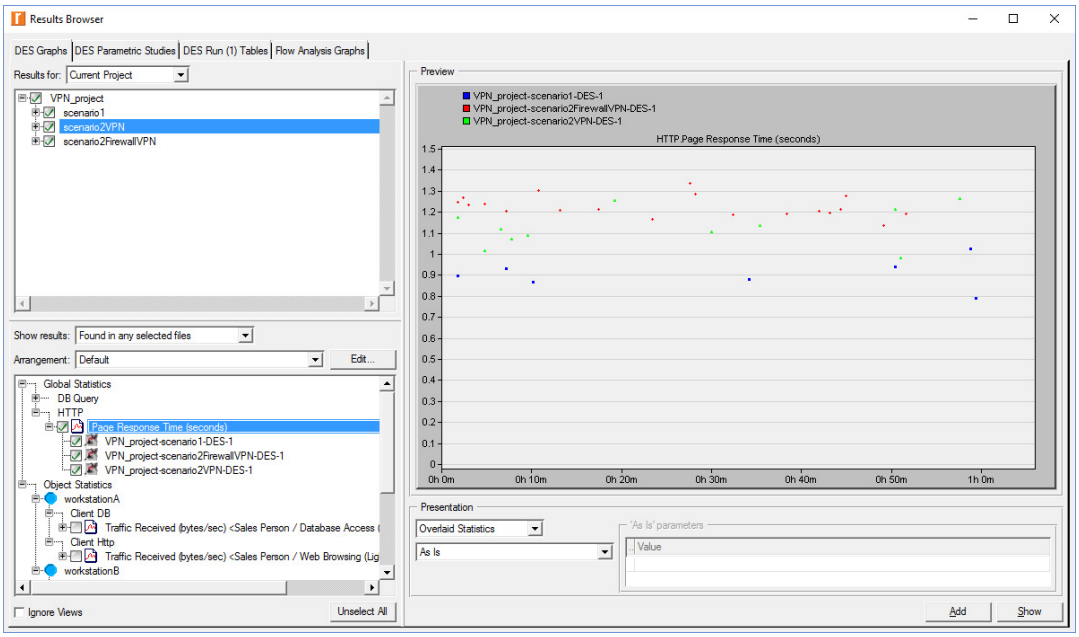
Global Statistics → HTTP · Page →Response Time (seconds) .

Παρακάτω φαίνονται οι χρόνοι απόκρισης για τα σενάρια

Με μπλε χρώμα το σενάριο χωρίς firewall και VPN

Με κόκκινο χρώμα το σενάριο με firewall

Με πράσινο χρώμα το σενάριο με firewall και VPN



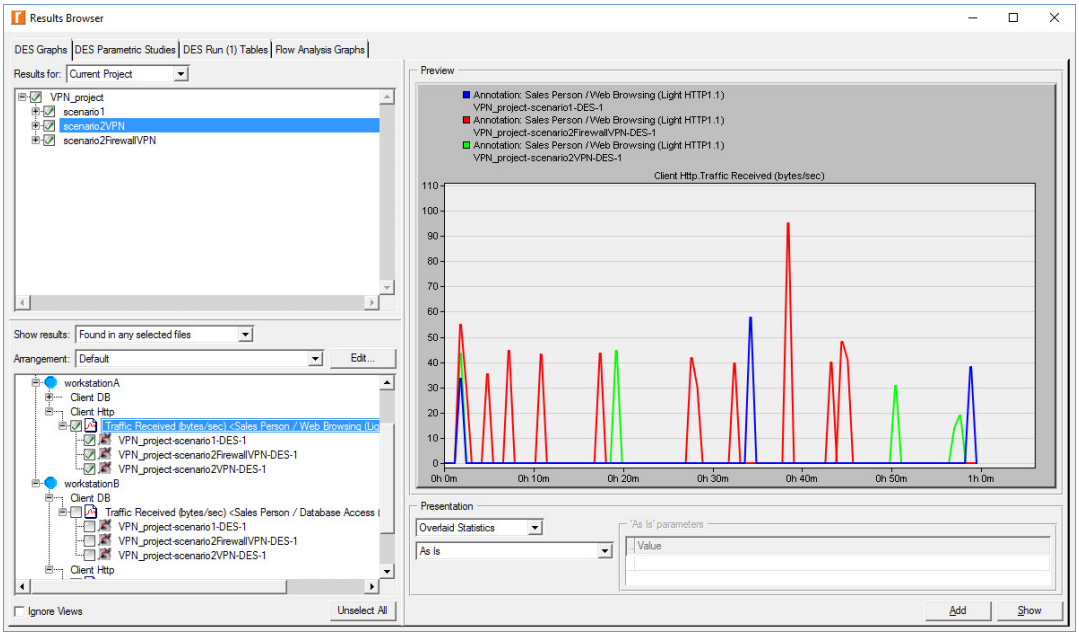
Στο σταθμό εργασίας:

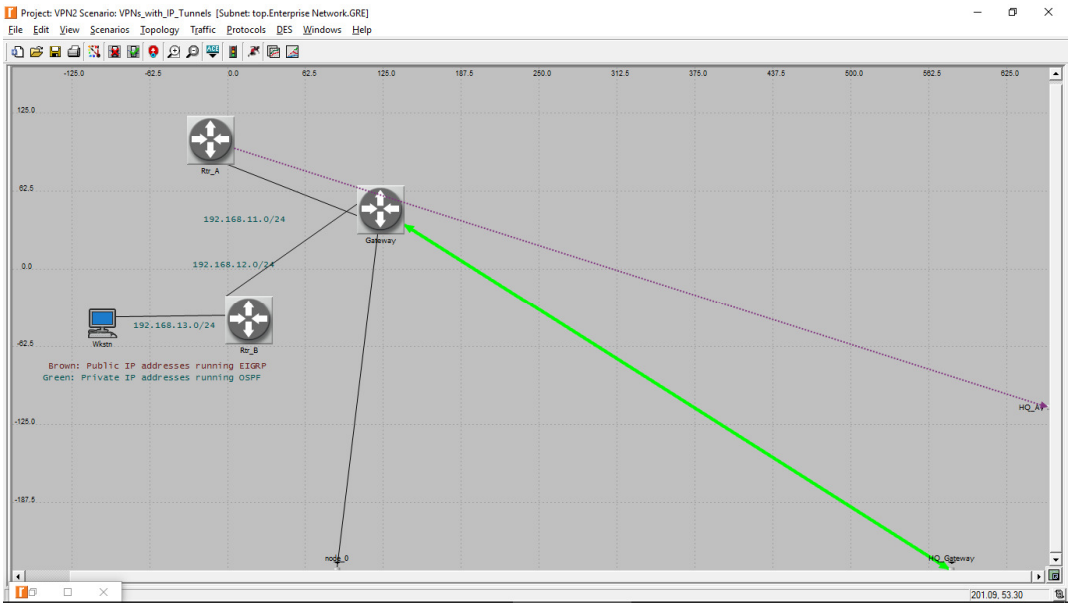
Client Http →Traffic Received (bytes/sec) .

Με μπλε χρώμα το σενάριο χωρίς firewall και VPN

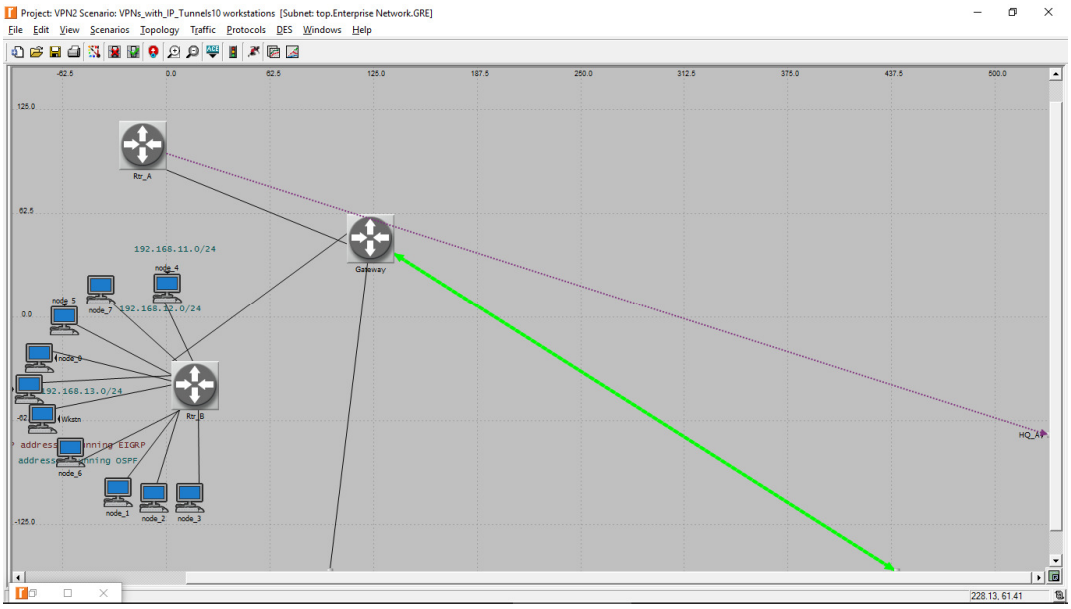
Με κόκκινο χρώμα το σενάριο με firewall

Με πράσινο χρώμα το σενάριο με firewall και VPN

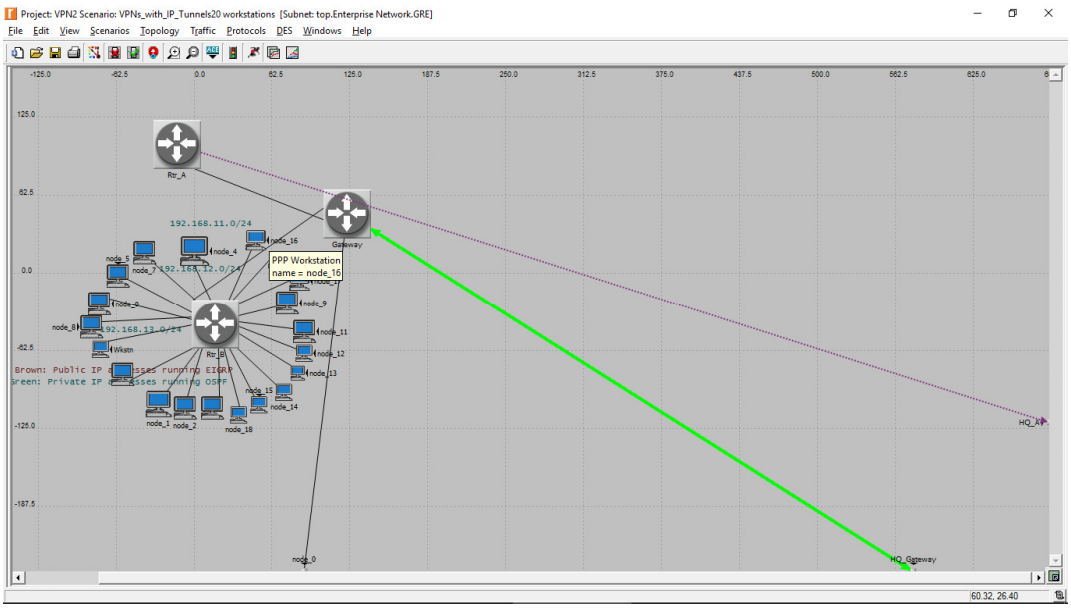




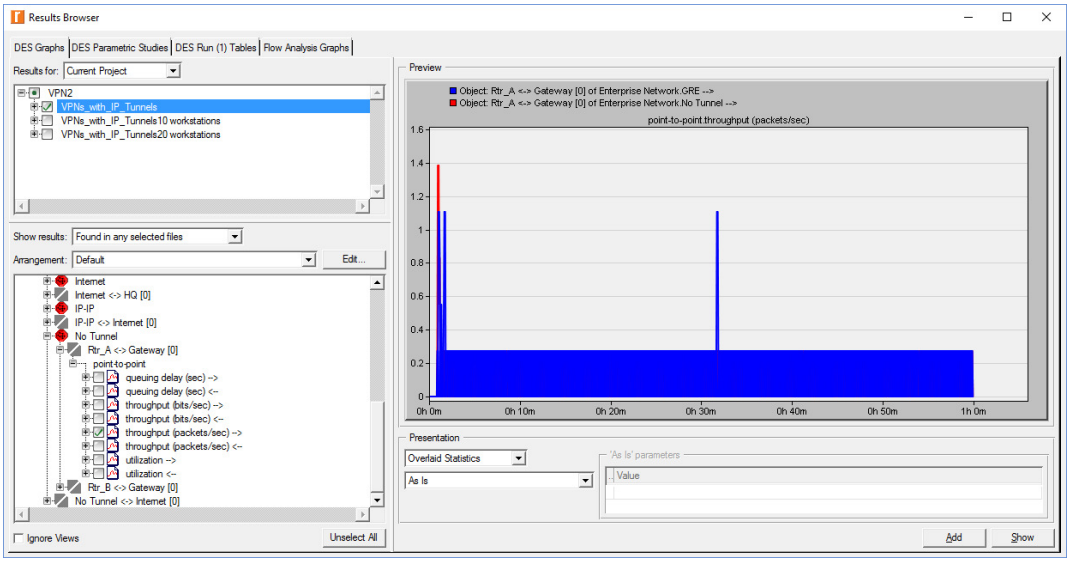
1 σταθμός εργασίας



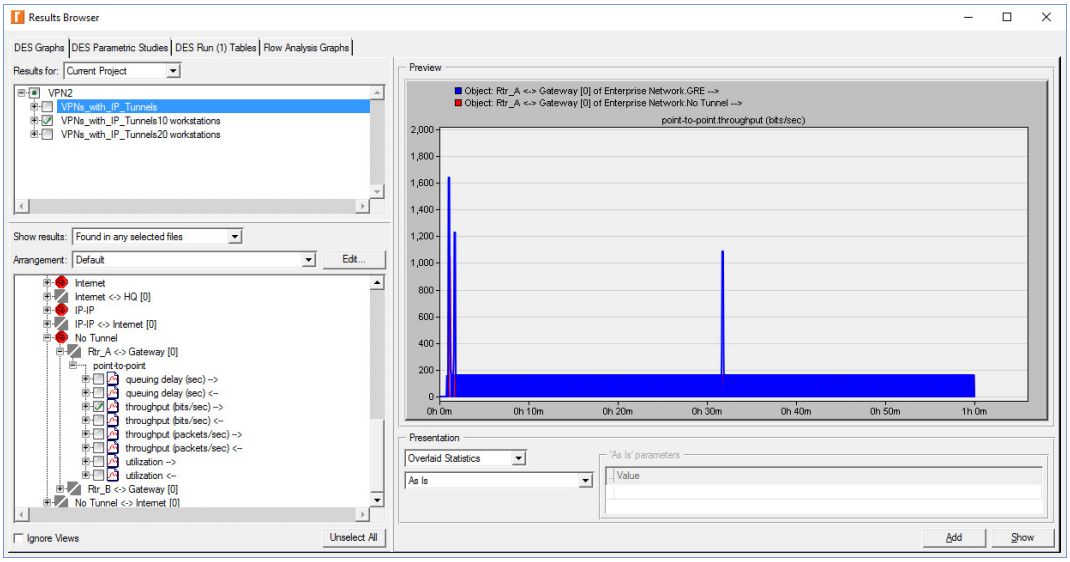
10 σταθμοί εργασίας



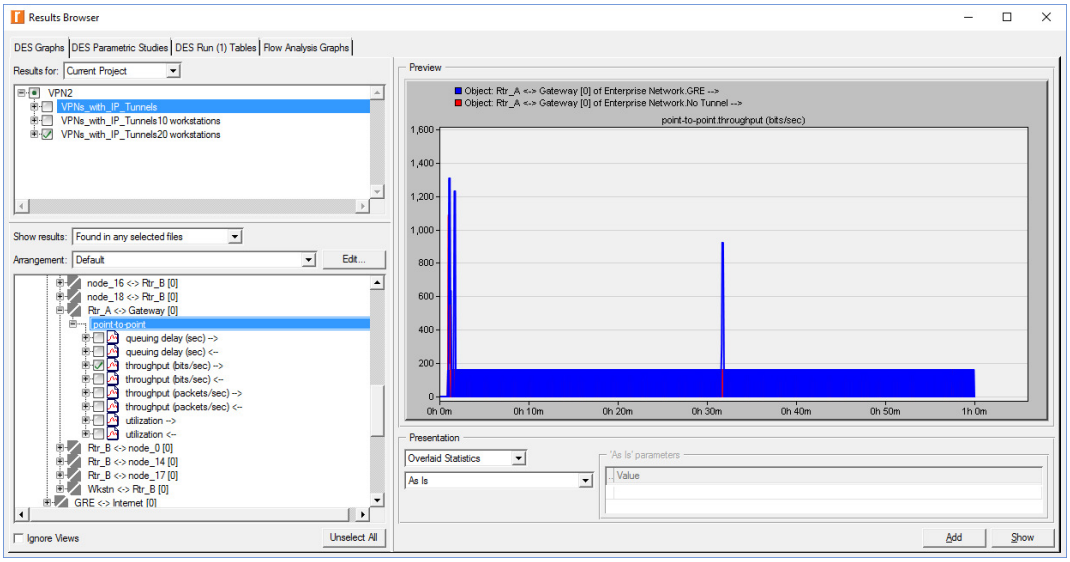
20 σταθμοί εργασίας



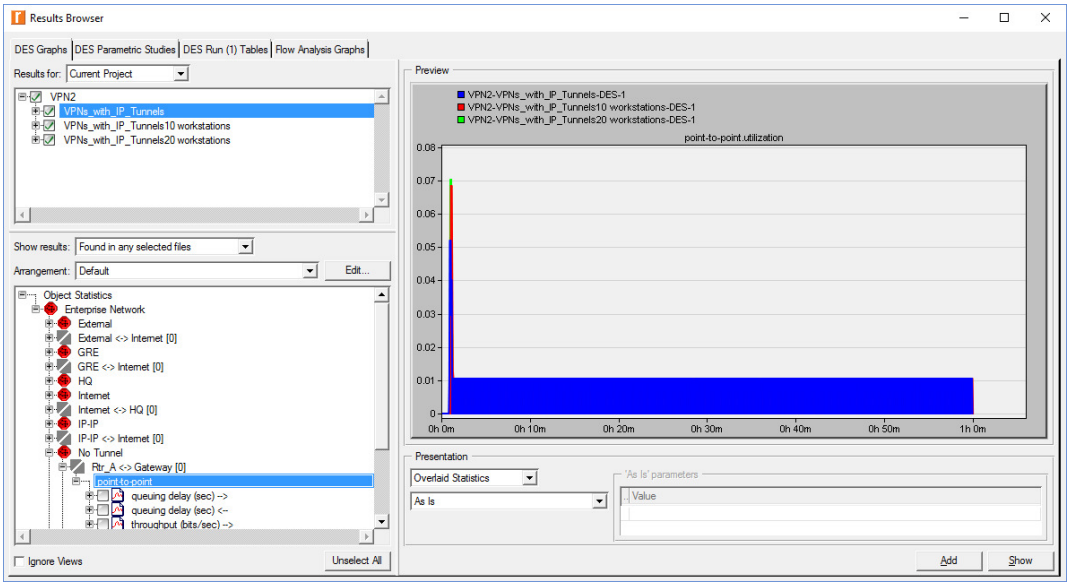
Packets/sec εξερχόμενα από τον gateway / router με και χωρίς IP tunneling για 1 σταθμό εργασίας



Bits /sec εξερχόμενα από τον gateway / router με και χωρίς IP tunneling για 10 σταθμούς εργασίας



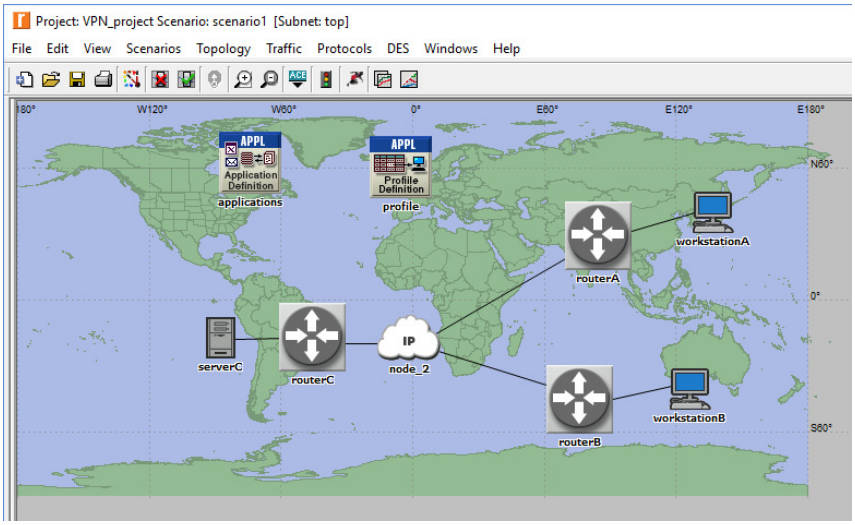
Bits /sec εξερχόμενα από τον gateway / router με και χωρίς IP tunneling για 20 σταθμούς εργασίας



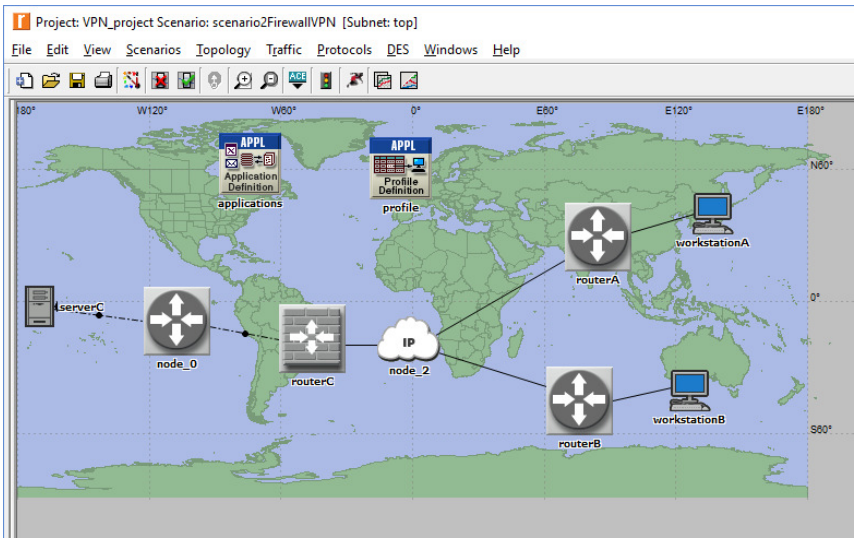
Σύγκριση χρήσης του router σε σχέση με το πλήθος των σταθμών εργασίας

Συμπεράσματα

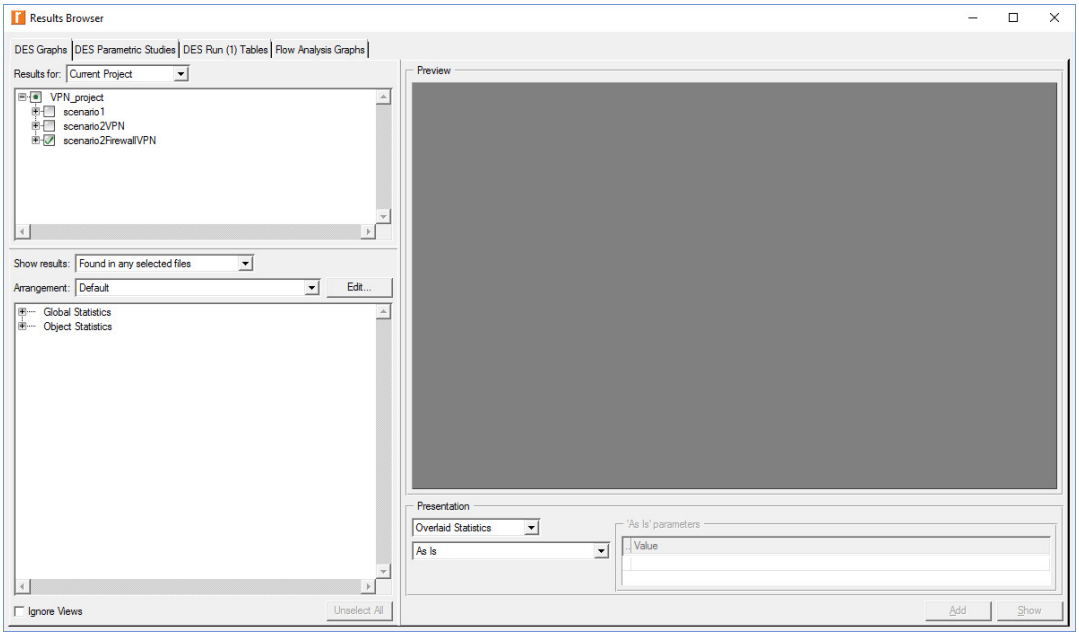
Στο σενάριο 1 η τοπολογία που χρησιμοποείται για την απλή μετάδοση δεδομένων περιέχει δύο σταθμούς εργασίας, οι workstationA και workstationB συνδέονται μέσω κάποιου router (routerA και routerB αντίστοιχα) στο internet. Επίσης υπάρχει ένας απομακρυσμένος server ο οποίος και αυτός είναι συνδεδεμένος στο διαδίκτυο μέσω του routerC.

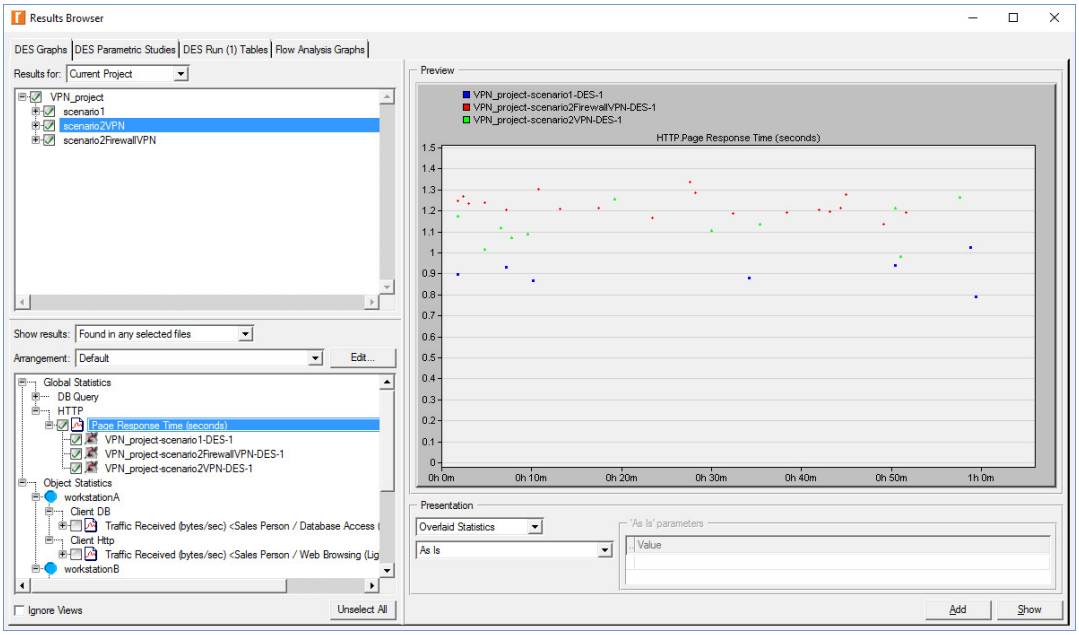


Στο δεύτερο σενάριο που αφορά στη σύνδεση VPN, ανάμεσα στον server και στον router C παρεμβάλλεται ένα επιπλέον router για την υλοποίηση του πρωτοκόλλου VPN. Η υλοποίηση γίνεται με τη χρήση MPLS VPN.

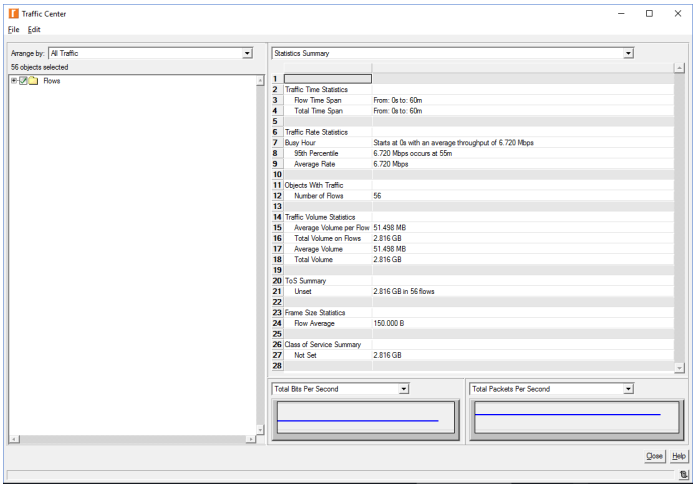


Στη συνέχεια για να συλλέξουμε τα δεδομένα επιλέγουμε Run Discrete Event Simulation και στη συνέχεια Compare Results από το Results menu.

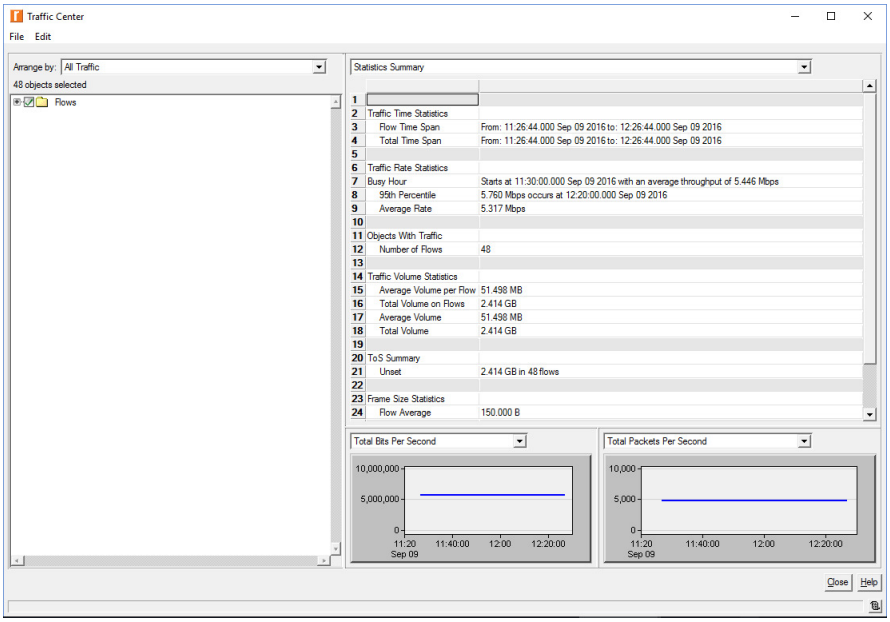




Έχοντας δημιουργήσει μια κίνηση τύπου IP Unicast στο σενάριο με απλή μετάδοση TCP/IP, παρατηρούμε ότι ο μέσος ρυθμός μετάδοσης είναι 6720 MBps.



Αντίστοιχα δημιουργώντας μια κίνηση τύπου IP Unicast στο σενάριο της VPN σύνδεσης παρατηρούμε ότι ο ρυθμός μετάδοσης είναι μειωμένος κατά 1403 MBps.



Η μείωση στο ρυθμό μετάδοσης είναι της τάξης του 20,8% και μάλιστα σε ένα σενάριο στο οποίο εμπλέκονται μόνο δύο clients. Ο βασικός λόγος για τον οποίο το VPN οδηγεί σε μείωση του ρυθμού μετάδοσης δεδομένων είναι το γεγονός ότι για να επιτευχθεί η ασφαλής επικοινωνία, τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται προσθέτουν επιπλέον επικεφαλίδες και συνεπώς δεδομένα στα ήδη υπάρχοντα πακέτα που πρόκειται να μεταδοθούν. Το IPsec πρωτόκολλο για παράδειγμα παράγει αρκετές επιπλέον επικεφαλίδες εξαιτίας των ποικίλων τεχνικών κρυπτογράφησης και ανταλλαγής δεδομένων που εμπλέκονται στην ασφαλή μετάδοση. Έτσι το πλήθος των bytes κατά τη μετάδοση της ίδιας πληροφορίας είναι πολύ μεγαλύτερο στην περίπτωση μιας VPN σύνδεσης από ότι στην περίπτωση της χρήσης απλού TCP/IP πρωτοκόλλου.

Επίσης στην περίπτωση μετάδοσης σε πολλούς clients η ταχύτητα μετάδοσης από έναν server μειώνεται δραματικά διότι απαιτείται μεγάλη υπολογιστική ισχύς από μέρους του server για την κωδικοποίηση με τη

χρήση πρωτοκόλλων κρυπτογράφησης. Αυτό σημαίνει ότι όσοι περισσότεροι είναι οι clients τόσο περισσότερο επιβαρύνεται ο VPN server με αποτέλεσμα σε περιπτώσεις αυξημένου φόρτου να παρατηρούνται καθυστερήσεις διότι ο server δεν μπορεί να ανταποκριθεί σε όλα τα αιτήματα.

Βιβλιογραφία

- Dovrolis C (2013) CS8803-NS Network Science Fall , Ανάκτηση από: http://www.cc.gatech.edu/~dovrolis/Courses/NetSci/ (30.1.2016)
- Furst K, Lang WW, Nolle DE (2002) Internet banking. J Financ Serv Res, Vol.22, No.12,pp.95–117
- Hoffman, P. (2005). *Cryptographic Suites for IPsec*. IETF. RFC 4308.
- Peterson P.,(2007), The new Banking services, McGraw Hill
- Richardson, M. (2005). *A Method for Storing IPsec Keying Material in DNS*. IETF. RFC 4025.
- Sommestad, T., Ekstedt, M., Holm, H., & Afzal, M. (2011). Security mistakes in information system deployment projects. Information Management & Computer Security, 19(2), 80-94.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.
- Stallings W. (2006) *Cryptography and Network Security*, Pearson Education, p. 492-493
- Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.
- Thimm, H., & Rasmussen, K. B. (2013). Obtaining informed ness in collaborative networks through automated information provisioning–a modelling framework and active database system approach. International Journal of Computer Integrated Manufacturing, 26(11), 1054-1065.
- Wang P., W. Hawk, and C. Tenopir. Users' interaction with world wide web resources: an exploratory study using a holistic approach. Inf. Process. Manage., 36:229{251, January 2000.
- Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.
- Xu, J., Chau, M., and Tan, C. Y. B., (2014), "The Development of Social Capital in the Collaboration Network of Information Systems Scholars", Journa of the Association of Informational Systems, vol. 15, Issue 12, pp. 835-859
- Yan, L., & Ma, Z. M. (2014). Modeling fuzzy information in fuzzy extended entity-relationship model

and fuzzy relational databases. Journal of Intelligent and Fuzzy Systems, 27(4), 1881-1896.

- Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. Human Resource Management Review, 23(1), 105-113.

- Γιαννόπουλος Γ.Ν.,(2001), Προστασία Προσωπικών Δεδομένων και διανοσυριακή ροή πληροφοριών, Τόμος 11, Εκδόσεις Σάκουλας, σελ. 733

- Nextep Broadband, "Virtual Private Networks - Solutions for cost-effective, high-speed corporate extranets and wide-area networks" White Paper May 2001

- International Engineering Consortium, www.iec.org
- Microsoft, "Virtual Private Networking in Windows 2000: An Overview" White Paper 1999
- Andreas Steffen, "Virtual Private Networks Coping with Complexity" Security Group, Zürcher Hochschule Winterthur 2003
- Nortel Networks, "Virtual Private Networks and IPsec", White Paper 2002